



PREPARING THE CYBER BATTLEFIELD: ASSESSING A NOVEL ESCALATION RISK IN A SINO-AMERICAN CRISIS

Ben Buchanan
Fiona S. Cunningham

Do cyber capabilities create novel risks of a future political crisis between the United States and China escalating into a conflict? This article outlines one potential pathway for interstate crises to escalate: the use of force in response to adversary hacking operations that could enable high-end cyber attacks. Often known as operational preparation of the environment or OPE, these acts lay the groundwork for future attacks but are difficult to distinguish from espionage. While some scholars argue that states might respond to the discovery of an intruder with the use of force, others have found little empirical evidence that cyber capabilities affect interstate conflict dynamics. To assess these competing claims, we examine Chinese and U.S. leadership views, organizational and operational practices for cyber conflict, and the bilateral cyber relationship. We conclude that the risk of inadvertent escalation due to cyber capabilities in a future Sino-American crisis cannot be dismissed.

In the context of rapidly deteriorating Sino-American relations, U.S. analysts are increasingly concerned that a political crisis between the two countries could escalate into an armed conflict. Since both countries began to develop cyber capabilities in the mid-2000s, scholars and analysts have warned that those capabilities could add incentives for either the United States or China to use force in a crisis. As Kurt Campbell and Ali Wyne wrote: “Continued advances in cyberoffensive capabilities that increase the risk of inadvertent escalation, potentially up to the nuclear level, make ... the deteriorating security environment in the Asia-Pacific even more concerning.”¹ Despite these concerns, scholars continue to debate whether offensive cyber capabilities create novel risks of great-power political crises escalating into conflicts. Cyber capabilities differ from conventional military capabilities and nuclear weapons in important ways. These differences create new

pathways through which a great-power crisis could escalate into a conventional conflict. But scholars have yet to find empirical evidence that states or individuals actually take those pathways.

This article examines one of these novel escalation pathways in the context of the Sino-American relationship: the difficulty of distinguishing between hacking for espionage and operational preparation of the environment (OPE), an essential precursor to most high-end cyber attacks. A state discovering that an adversary has exploited its computer networks will often struggle to discern why that adversary has done so. On the one hand, the intruders might be performing espionage, including the collection of intelligence to better defend their own networks. On the other hand, the intruders may be performing OPE to enable a cyber attack. Intrusions for either purpose are often indistinguishable to the network’s operator.

As most cyber attacks need OPE to be successful, this OPE-espionage distinction problem cre-

1 Kurt M. Campbell and Ali Wyne, “The Growing Risk of Inadvertent Escalation Between Washington and Beijing,” *Lawfare*, Aug. 16, 2020, <https://www.lawfareblog.com/growing-risk-inadvertent-escalation-between-washington-and-beijing>.

ates pathways for inadvertent escalation in a crisis. A state could correctly detect an adversary's OPE and, fearing an imminent cyber attack with severe consequences, choose to use force first, escalating the conflict with a cyber or even kinetic attack. But a state could also misperceive an adversary's efforts to collect intelligence via cyber means as preparation to conduct a cyber attack and preempt that attack with conventional or cyber attacks of its own.² Analysts are particularly concerned about a scenario in which a state discovers during a crisis that its adversary has intruded into its nuclear command, control, and communications networks.³ Despite these concerns, academic studies based on observational data, surveys, and simulations find little correlation between cyber attacks and escalation, either in peacetime or during conflicts.⁴ Scholars have reasoned that most cyber attacks are simply not destructive enough to worsen crisis or conflict outcomes.⁵ These limited effects, coupled with the bloodless, secret nature of cyber attacks, might instead open up new pathways for de-escalation.⁶

In an attempt to evaluate the concerns of the U.S. policy community and the ongoing scholarly

debates on cyber escalation in great-power crises, this article examines the escalation risks created by cyber capabilities, and OPE in particular, in a future crisis scenario involving the United States and China. The external validity of existing empirical findings to military crises among great powers is limited because no such crisis has occurred in the past two decades and these situations are difficult to replicate in surveys and simulations with U.S. participants.⁷ A Sino-American crisis scenario is a most likely case for theoretical claims that cyber capabilities create novel escalation risks. Both countries would be more likely to react to any independent effect of cyber technology on their incentives to use force, if such incentives exist, than they might in non-crisis situations where political and strategic factors could extinguish those incentives.

A Sino-American crisis scenario involving Taiwan, North Korea, or territorial disputes in the East China Sea and South China Sea could plausibly spill over into armed conflict. Scholars have pointed to a number of reasons that a Sino-American conflict could escalate that are not specific to cyber operations.⁸ They have also argued that cyber capabilities

2 See for example, Martin Libicki, *Crisis and Escalation in Cyberspace* (Santa Monica, CA: RAND Corporation, 2012); Herbert Lin, "Escalation Dynamics and Conflict Termination in Cyberspace," *Strategic Studies Quarterly* 6, no. 3 (Fall 2012): 46–70, <https://www.jstor.org/stable/26267261>.

3 See for example, James M. Acton, "Cyber Warfare & Inadvertent Escalation," *Daedalus* 149, no. 2 (Spring 2020): 133–149, https://doi.org/10.1162/daed_a_01794; Erik Gartzke and Jon R. Lindsay, "The Cyber Commitment Problem and the Destabilization of Nuclear Deterrence," in *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*, ed. Herbert Lin and Amy Zegart (Washington, DC: Brookings Institution Press, 2019), 195–234.

4 Brandon Valeriano and Ryan Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System* (New York, NY: Oxford University Press, 2015), chap. 5; Nadiya Kostyuk and Yuri M. Zhukov, "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?" *Journal of Conflict Resolution* 63, no. 2 (November 2017): 317–347, <https://doi.org/10.1177/2F0022002717737138>; Jacquelyn G. Schneider, "The Information Revolution and International Stability: A Multi-Article Exploration of Computing, Cyber, and Incentives for Conflict" (Ph.D. diss., George Washington University, 2017), 119; Sarah Kreps and Jacquelyn Schneider, "Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving beyond Effects-Based Logics," *Journal of Cybersecurity* 5, no. 1 (2019): 8–9, <https://doi.org/10.1093/cybsec/tyz007>.

5 Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security* 38, no. 2 (Fall 2013): 41–73, https://doi.org/10.1162/ISEC_a_00136; Erica D. Borghard and Shawn W. Loneragan, "The Logic of Coercion in Cyberspace," *Security Studies* 26, no. 3 (2017): 476–8, <https://doi.org/10.1080/09636412.2017.1306396>; Erica D. Borghard and Shawn W. Loneragan, "Cyber Operations as Imperfect Tools of Escalation," *Strategic Studies Quarterly* (Fall 2019): 122–45, <https://www.jstor.org/stable/26760131>; Brandon Valeriano, Benjamin M. Jensen, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (New York, NY: Oxford University Press, 2018).

6 Valeriano, Jensen, and Maness, "Cyber Strategy"; Joshua Rovner, "Cyber War as an Intelligence Contest," *War on the Rocks*, Sept. 16, 2019, <https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/>.

7 For a useful discussion of the external validity of surveys and simulations, see, Kreps and Schneider, "Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains," 9; Schneider, "The Information Revolution and International Stability," 122–30.

8 Those reasons include differing perceptions of the status quo, differing U.S. and Chinese beliefs about escalation, inattention to inadvertent escalation risks, inattention to escalation risks due to relatively moderate levels of tension in the relationship compared to the Cold War, tensions between crisis management and warfighting objectives, and the employment of military capabilities with multiple roles. See, James M. Acton, "Escalation Through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War," *International Security* 43, no. 1 (Summer 2018): 89–92, https://doi.org/10.1162/isec_a_00320; Thomas J. Christensen, "The Meaning of the Nuclear Evolution: China's Strategic Modernization and US-China Security Relations," *Journal of Strategic Studies* 35, no. 4 (2012): 482–484, <https://doi.org/10.1080/01402390.2012.714710>; Fiona S. Cunningham and M. Taylor Fravel, "Assuring Assured Retaliation: China's Nuclear Strategy and U.S.-China Strategic Stability," *International Security* 40, no. 2 (Fall 2015): 7–50, https://doi.org/10.1162/ISEC_a_00215; Fiona S. Cunningham and M. Taylor Fravel, "Dangerous Confidence? Chinese Views of Nuclear Escalation," *International Security* 44, no. 2 (2019): 61–109, https://doi.org/10.1162/isec_a_00359; Avery Goldstein, "First Things First: The Pressing Danger of Crisis Instability in U.S.-China Relations," *International Security* 37, no. 4 (Spring 2013): 79–62, https://doi.org/10.1162/ISEC_a_00114; Alastair Iain Johnston, "The Evolution of Interstate Security Crisis-Management Theory and Practice in China," *Naval War College Review* 69, no. 1 (Winter 2016): 28–71, <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1118&context=nwc-review>; Joshua Rovner, "Two Kinds of Catastrophe: Nuclear Escalation and Protracted War in Asia," *Journal of Strategic Studies* 40, no. 5 (2017): 696–730, <https://doi.org/10.1080/01402390.2017.1293532>; Caitlin Talmadge, "Would China Go Nuclear? Assessing the Risk of Chinese Nuclear Escalation in a Conventional War with the United States," *International Security* 41, no. 4 (Spring 2017): 50–92, https://doi.org/10.1162/ISEC_a_00274; Zhao Tong and Li Bin, "The Underappreciated Risks of Entanglement: A Chinese Perspective," in *Entanglement: Russian and Chinese Perspectives on Non-Nuclear Weapons and Nuclear Risks*, ed. James M. Acton (Washington, DC: Carnegie Endowment for International Peace, 2017), 59–63; Adam Segal, "U.S. Offensive Cyber Operations in a China-U.S. Military Confrontation," in *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*, ed. Herbert Lin and Amy Zegart (Washington, DC: Brookings Institution Press, 2019), 319–41.

could contribute to Sino-American crisis instability, due to the difficulty of distinguishing OPE for cyber attacks from espionage, pressures on decision-makers to use force before military networks are degraded, operators accidentally damaging each other's networks, or mistaken attribution of cyber attacks conducted by third parties.⁹ But existing analysis of the contribution of OPE to Sino-American crisis escalation is relatively superficial.¹⁰

To thoroughly assess the escalation risks posed by the problem of distinguishing OPE and cyber-enabled espionage in a Sino-American crisis, this paper follows the approach of existing scholarship that attempts to assess the risk of escalation in future Sino-American crisis and conflict scenarios. Given the scarcity and imperfection of available sources, especially on the Chinese side, our findings are necessarily tentative but do provide a more comprehensive assessment of the escalation risks than existing scholarship. No military crisis has occurred since both states developed offensive cyber capabilities in the mid-2000s.¹¹ We therefore examine the two countries' leadership statements, threat perceptions, procedures for authorizing cyber operations, organizational structures, capabilities, and policies for evidence that they create, recognize, and seek to manage escalatory risks. We also consider features of the bilateral relationship that could exacerbate or mitigate the risks of cyber capabilities contributing to crisis instability, such as mechanisms for crisis communication.

Our analysis provides evidence that inadvertent escalation risks associated with OPE would be present in a future Sino-American crisis scenario. But leaders from both countries might choose to avoid those pathways. Official U.S. policy for offensive cyber operations recognizes the escalation risks associated with cyber espionage being mistaken for OPE, but the United States has recently made changes to its cyber strategy that may increase these risks. Meanwhile, Chinese writings recognize the difficulty of distinguishing between cyber attacks and OPE but do not discuss the es-

calation risks resulting from that difficulty. We also find that three aspects of the Sino-American cyber relationship add to the likelihood of the two countries misperceiving each other's behavior: an asymmetry in the relative maturity of U.S. and Chinese cyber doctrine and cyber capabilities, dim prospects for official dialogue that could improve mutual understanding of each other's cyber operations, and the absence of a crisis communications mechanism specific to cyberspace. We acknowledge that our empirical evidence could support the claim that cyber technology does not create inadvertent escalation risks, but we do not draw this conclusion. We found no evidence that China has carefully assessed these escalation risks. Nor are we confident that the United States has parsed the independent effect of cyber technology from other incentives that U.S. adversaries face not to use force in its assessments of those risks.

These issues are important to both scholars and policymakers for a variety of reasons. First, we aim to contribute to the debate about the escalation risks created by cyber operations by examining a scenario in which cyber capabilities are expected to contribute to the use of force.¹² Second, we provide evidence of Chinese views with which to assess the escalatory potential of cyber operations. Evidence from China is missing from existing policy debate and scholarly research about cyber conflict, which draws heavily on U.S. experiences, perspectives, and participants. Third, these questions are relevant to policymakers in both countries who manage the risks of cyber escalation, especially as Sino-American tensions increase.

We begin with a brief explanation of OPE as a distinctive feature of cyber attacks. The second section outlines the competing hypotheses about cyber escalation in existing scholarly literature and the mechanisms that could link detection of an intrusion in a crisis with the decision to use force. The third, fourth, and fifth sections examine the evidence for these hypotheses in U.S. documents and statements, Chinese writings and organiza-

9 David C. Gompert and Martin Libicki, "Cyber Warfare and Sino-American Crisis Instability," *Survival* 56, no. 4 (September 2014): 7–22, <https://doi.org/10.1080/00396338.2014.941543>; Ariel (Eli) Levite and Lyu Jinghua, "Chinese-American Relations in Cyberspace: Toward Collaboration or Confrontation?" *China Military Science*, Jan. 24, 2019, <https://carnegieendowment.org/2019/01/24/chinese-american-relations-in-cyberspace-toward-collaboration-or-confrontation-pub-78213>; Segal, "U.S. Offensive Cyber Operations in a China-U.S. Military Confrontation."

10 Gompert and Libicki, "Cyber Warfare and Sino-American Crisis Instability," 13; Acton, "Escalation Through Entanglement"; Zhao and Li, "The Underappreciated Risks of Entanglement," 320.

11 The last serious bilateral crisis occurred in 2001 when a Chinese fighter aircraft collided with a U.S. EP-3 spy plane conducting surveillance over the South China Sea.

12 For key contributions to that debate, see, Libicki, *Crisis and Escalation in Cyberspace*; Kreps and Schneider, "Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains"; Valeriano and Maness, *Cyber War Versus Cyber Realities*; Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, no. 3 (2013): 365–404, <https://doi.org/10.1080/09636412.2013.816122>; Gartzke, "The Myth of Cyberwar"; Borghard and Loneragan, "The Logic of Coercion in Cyberspace"; Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (Winter 2016): 44–71, https://doi.org/10.1162/ISEC_a_00266; Erik Gartzke and Jon R. Lindsay, "Coercion Through Cyberspace: The Stability-Instability Paradox Revisited," in *Coercion: The Power to Hurt in International Politics*, ed. Kelly M. Greenhill and Peter Krause (New York, NY: Oxford University Press, 2018), 179–203.



tional practices, and the bilateral cyber relationship, respectively. The sixth section evaluates the escalation risks and provides policy recommendations to mitigate them.

Operational Preparation of the Environment

Many cyber operations are governed by a simple fact: In order to develop a cyber capability with a potent or customized effect on a target network, substantial reconnaissance and preparation are required from within that targeted network. In 2010, the Department of Defense defined “Cyber Operations in Preparation of the Environment” as:

Non-intelligence enabling functions within cyberspace conducted to plan and prepare for potential follow-up military operations. [Cyber-OPE] includes but is not limited to identifying data, system/network configurations, or physical structures ... for the purpose of determining system vulnerabilities; and actions taken to assure future access and/or control of the system, network, or data during anticipated hostilities.¹³

While cyber OPE has some analogues in other forms of military operations — especially in the world of special operations and covert action — it differs from operations that are more familiar to policymakers, such as conventional and nuclear operations. Some military capabilities for these purposes also require substantial preparation, but that activity can take place mostly within a state’s own territory. The research, development, production, and testing of nuclear weapons and their delivery systems have multiyear lead times, but this is usually done at home.¹⁴ Similar dynamics apply to a state’s development of cruise mis-

siles, bombers, tanks, and other military hardware. While peacetime reconnaissance is fundamental to many kinds of military operations,¹⁵ preparations to use cyber capabilities have different reconnaissance requirements than most other operations.¹⁶ Cyber operations differ from these other types of military capabilities and operations. Much of the development and preparation for a cyber operation requires access to or occurs within adversary networks. Moreover, the accesses and payloads that make offensive cyber operations possible are often specific to a particular network: Cyber operations lack the fungibility of conventional or nuclear weapons and should be tailored to their targets in order to be effective.¹⁷

Contrary to the view that destructive cyber attacks on an enemy’s networks are easy to carry out once those networks are penetrated, the effectiveness of an attack is heavily dependent on the attacker’s OPE.¹⁸ Nor is gaining access to an adversary’s networks a simple task. Gaining and maintaining access to a target network is generally difficult, resource intensive, and specific to the target network.¹⁹ The effects of an attack, the ability to sustain those effects over time, and the ability of an attack to limit unintended consequences all depend on how well the attacker has prepared and understood the target network and the likely actions of the network’s defenders once the attack commences.²⁰

A few examples illustrate the importance of OPE to sophisticated offensive cyber operations. Stuxnet, the most famous cyber attack in history, was enabled by months if not years of reconnaissance. Kaspersky, a major cyber security firm, found evidence that the attack code of Stuxnet was preceded by code that enabled substantial espionage efforts against Iranian targets. The information from these espionage efforts was used to inform the development of the Stuxnet code, which manipulated the Iranian centrifuges in very specific ways. Espionage and preparation carried out within the Irani-

13 Vice Chairman of the Joint Chiefs of Staff, Department of Defense, “Memorandum: Subject: Joint Terminology for Cyberspace Operations,” 2010, 7, from “The United States and Cyberspace: Military Organization, Policies, and Activities,” Document 10, *National Security Archive*, Jan. 20, 2016, <https://nsarchive.gwu.edu/briefing-book/cyber-vault/2016-01-20/united-states-cyberspace-military-organization-policies-activities>.

14 Some states have tested nuclear weapons outside of their homelands, but they generally do so in outlying territories (e.g., French and U.S. tests in their Pacific territories) or on the territory of allies (e.g., U.K. nuclear tests in Australia).

15 See for example, Stephen Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle* (Princeton, NJ: Princeton University Press, 2004), 63.

16 For a helpful comparison of the intelligence requirements for nuclear and offensive cyber operations, see, Austin Long, “A Cyber SIOP?” in *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*, ed. Herbert Lin and Amy Zegart (Washington, DC: Brookings Institution Press, 2019), 116–22.

17 Long, “A Cyber SIOP?” 121.

18 For discussion of this principle and examples, see, Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations* (Oxford: Oxford University Press, 2016), chap. 2.

19 Borghard and Loneragan, “Cyber Operations as Imperfect Tools of Escalation,” 126.

20 Lin, “Escalation Dynamics and Conflict Termination in Cyberspace,” 50–51.

an network made the Stuxnet attack possible, but the preparation that enabled Stuxnet was useful almost exclusively for an attack against Iran.²¹ The Stuxnet code could not be used to attack North Korean centrifuges, for example.

The blackouts in Ukraine in 2015 and 2016 provide further evidence of the reconnaissance requirements for major cyber attacks on critical civilian infrastructure. These are vitally important cases to study, as they offer the only two public

The 2016 attack was even more notable, as it featured customized malicious code that, due to the attackers' understanding of the industrial control systems in Ukraine, enabled more scalable and automated attacks on power systems.²³

Overall, the general pattern is clear: Performing OPE is essential to enabling more powerful cyber operations that offer more lasting geopolitical value.²⁴ A drumbeat of other attacks bears out this trend. Iranian hackers spent months inside the computer networks of Sands Casino and Saudi Aramco before they attacked in 2012.²⁵ North Korean hackers did the same with their attacks on the computer networks of Sony Pictures.²⁶ Russian hackers prepared in a similar way for their NotPetya operation, perhaps the most devastating cyber attack in history, with reports of over \$10 billion in damage.²⁷ Some attacks, most notably denial-of-service efforts, do not fit into this trend.

Overall, the general pattern is clear: Performing OPE is essential to enabling more powerful cyber operations that offer more lasting geopolitical value. A drumbeat of other attacks bears out this trend.

instances in which a cyber attack managed to turn off the power to hundreds of thousands of people. OPE made both attacks possible. A detailed after-action review of the 2015 attack on Ukraine concluded:

The strongest capability of the attackers was not in their choice of tools or in their expertise, but in their capability to perform long-term reconnaissance operations required to learn the environment and execute a highly synchronized, multistage, multisite attack.²²

But they are remarkable for their overall lack of potency. For example, the Iranian attacks on the U.S. banking sector in 2012 did not require OPE but also did not pack much punch.²⁸

In addition to occurring within an adversary's networks, OPE is difficult to distinguish from espionage once it is discovered by a target. In theory, there might be ways for a target to tell whether an intrusion is espionage or whether it facilitates an attack. But there are no foolproof solutions to this OPE-espionage distinction problem. For example, an uptick in communication between the attacker and malicious code implanted in the target sys-

21 See, "A Fanny Equation: 'I Am Your Father, Stuxnet,'" *Kaspersky Lab*, Feb. 17, 2015, <https://securelist.com/a-fanny-equation-i-am-your-father-stuxnet/68787/>. For more on Stuxnet, see, Kim Zetter, *Countdown to Zero Day* (New York, NY: Crown, 2014); Lindsay, "Stuxnet and the Limits of Cyber Warfare."

22 Robert Lee, Michael Assante, and Tim Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid," *Electricity Information Sharing and Analysis Center*, March 18, 2016, 2.

23 "CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations," Dragos, <https://www.dragos.com/wp-content/uploads/Crash-Override-01.pdf>; Michael J. Assante, Robert M. Lee, and Tim Conway, "ICS Defense Use Case No. 6: Modular ICS Malware," *Electricity Information Sharing and Analysis Center*, Aug. 2, 2017, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_6.pdf; Anton Cherepanov, "Industroyer: Biggest Threat to Industrial Control Systems since Stuxnet," *ESET*, June 12, 2017, <https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/>; Greg Masters, "Industroyer Can Knock out Power Grid, ESET," *SC Magazine*, June 12, 2017, <https://www.scmagazine.com/home/security-news/malware/industroyer-can-knock-out-power-grid-eset/>.

24 Thomas Rid and Peter McBurney, "Cyber-Weapons," *RUSI Journal* 157, no. 1 (2012): 6–13, <https://doi.org/10.1080/03071847.2012.664354>; Lin, "Escalation Dynamics and Conflict Termination in Cyberspace," 50–51.

25 Ben Elgin and Michael Riley, "Now at the Sands Casino: An Iranian Hacker in Every Server," *Bloomberg*, Dec. 11, 2014, <https://www.bloomberg.com/news/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas>; Chris Kubecka, "How to Implement IT Security after a Cyber Meltdown," *YouTube*, Dec. 29, 2015, https://www.youtube.com/watch?v=WyMobr_TDSI.

26 "United States of America v. Park Jin Hyok," Department of Justice, June 8, 2018, 45–53, from "Cyber Brief: DOJ's Park Jin Hyok Criminal Complaint and North Korean Cyber Operations," *National Security Archive*, Sept. 6, 2018, <https://nsarchive.gwu.edu/news/cyber-vault/2018-09-06/cyber-brief-doj-park-jin-hyok-criminal-complaint-north-korean-cyber-operations>.

27 Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, Aug. 22, 2018, <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>.

28 "United States of America v. Ahmad Fathi, Hamid Firoozi, Amin Shokohi, Sadegh Ahmadzadegan, Omid Ghaffarinia, Sina Keissar, and Nader Saedi," Department of Justice, March 24, 2016, <https://www.justice.gov/opa/file/834996/download>.



tem could signal its purpose, but an attack could occur without any of those signals. Those signals could also accompany routine intelligence collection.²⁹ Even if an attacker tries to use those signals to distinguish OPE from espionage, the target may not receive those signals or treat them as credible.³⁰ The nature of the target network may provide some hints — for example, critical infrastructure industrial control systems are more likely to be exploited for OPE than intelligence gathering — but this is not always the case.³¹

EVEN IF THE INTRUDER SOUGHT TO REASSURE THE TARGET OF ITS INTENT NOT TO USE THE INTRUSION TO ENABLE AN ATTACK, IT PROBABLY COULD NOT DO SO. A HACK BEGUN WITH ONE INTENT IS ABLE TO SHIFT PURPOSES TO SERVE ANOTHER, UNDERMINING THE CREDIBILITY OF SUCH ASSURANCES.

A final noteworthy feature of OPE is that exploitation of an adversary's networks for intelligence gathering could be repurposed for OPE without any telltale signs that the target might detect. An operation that begins with the goal of collecting general intelligence could quickly and silently shift to collecting intelligence that would be useful for carrying out a specific attack. In addition, an operation that begins solely as an espionage operation could use the same access to wipe key files on the targeted network. For example, there is some evidence to suggest that the first blackout in Ukraine began with an espionage objective and only later morphed into an attack operation.³²

The Novel Escalation Risks of OPE

How and why could an intrusion discovered in the midst of a crisis between two great powers create incentives for the use of force? How and why might decision-makers choose to use force when faced with those incentives?

We define a crisis as “a confrontation between two states involving a serious threat to vital national interests for both sides in which there is the expectation of a short time for resolution, and in which there is understood to be a sharply increased risk of war.”³³ We define escalation as “an increase in the intensity or scope of conflict that crosses threshold(s) considered significant by one or more of the participants.”³⁴ In the context of a great-power crisis, escalation involves the use of force, with either cyber or kinetic attacks.³⁵ We use the term “cyber escalation risks” to refer to an increase in the likelihood of a use of force in a great-power crisis due to the nature of cyber technology.

The existing literature on cyber conflict suggests four possible pathways between the discovery of an intrusion and the use of force. If decision-makers discover an intrusion into their key military or civilian networks during a crisis, most scholars agree that those decision-makers could not rule out the possibility that the intrusion enables OPE. But scholars disagree on whether decision-makers face incentives to escalate the crisis in response to that discovery. Whether the discovery of an intrusion would lead to the use of force depends on how decision-makers assess the seriousness of the threat posed by the intrusion and whether the state also has strategic or political incentives to use force. These four possibilities are captured in two “escalation hypotheses” that expect the use of force and two “de-escalation hypotheses” that do not expect the use of force.

First, *inadvertent escalation* could occur if the state assesses that the intrusion poses a serious threat and uses force in response to preempt, warn, punish, or deny the adversary the benefit of using its intrusion to conduct an attack. Sec-

29 Martin C. Libicki, “Drawing Inferences from Cyber Espionage,” *CyCon X: Maximizing Effects*, 10th International Conference on Cyber Conflict, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, 2018, <https://ccdcoe.org/uploads/2018/10/Art-06-Drawing-Inferences-from-Cyber-Espionage.pdf>, 4–6.

30 Libicki, “Drawing Inferences from Cyber Espionage,” 4–6.

31 Buchanan, *The Cybersecurity Dilemma*, chaps. 3 and 8.

32 Kim Zetter, “Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid,” *Wired*, March 3, 2016, <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>.

33 Goldstein, “First Things First,” 51.

34 Forrest E. Morgan, Karl P. Mueller, Evan S. Medeiros, Kevin L. Pollpeter, and Roger Cliff, *Dangerous Thresholds: Managing Escalation in the 21st Century* (Santa Monica, CA: RAND Corporation, 2008), xi.

35 For a definition of a “use of force” in cyberspace, see, Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable Cyber Operations*, 2nd edition (New York, NY: Cambridge University Press, 2017), 333–7.

ond, *deliberate escalation* could occur if the state decides to use force in response to the intrusion because of the combination of the threat posed by the intrusion and additional political and strategic incentives to escalate. The state would ignore the threat posed by the intrusion if not for those other incentives. Third, the state might assess that even if the intrusion is OPE and enables the adversary to carry out a cyber attack, the threat posed by that attack is *bluster* rather than a serious threat. In this situation, decision-makers would choose not to use force. Fourth, the state could assess that the intrusion would enable the adversary to carry out a cyber attack that does pose a serious threat but decide not to use force because of *countervailing* strategic and political incentives.

Below we outline the mechanisms of intrusion detection and assessment of intent shared by all four pathways. We then describe the logic underpinning the inadvertent escalation hypothesis in detail because it makes the strongest claims about the independent contribution of cyber technology to the use of force. It also best represents the concerns in current U.S. policy debates about the destabilizing effect of cyber technology in a future Sino-American crisis. Lastly, we briefly describe the arguments of the other three hypotheses, highlighting how their causal claims differ from the inadvertent escalation hypothesis.

Intrusion Detection in a Crisis

The scenario in which OPE could trigger the use of force in a crisis would likely begin months if not years before the crisis. The state that desires the option to carry out offensive cyber operations in a future conflict against important adversary military or civilian networks, such as a regional joint military command network, would conduct OPE during peacetime. Beginning OPE once a crisis has begun is almost certainly too late to complete the complex, time-consuming task.³⁶ The defenders of the target network may even be aware of the attacker's presence in the network in peacetime and try unsuccessfully to expel it.

Once a political crisis began — over an accidental collision between two rivals' military aircraft, for example — decision-makers in both states would

have to decide whether to back down, bargain diplomatically, or initiate a conflict to bargain with force. During their deliberations, the target state's decision-makers might discover their adversary's intrusions into important computer networks, including those that might be OPE. Such discoveries are more likely in a crisis because states anticipate espionage and attacks in that context, and will step up network defenses accordingly.³⁷ Those leaders would then assess the threat posed by each intrusion and decide whether and how to respond to it.

Challenges for Assessing Intent

Three features of offensive cyber operations complicate the task of the target's decision-makers charged with assessing the intent behind the intrusion: the OPE-espionage distinction problem, incentives for the intruder not to send signals of intent, and the inability of the intruder to send credible signals of intent. Faced with these uncertainties in the midst of a crisis, the target's decision-makers might decide it is most prudent to treat the intrusion as OPE, which creates an incentive to use of force if they believe that the intrusion poses a serious threat.

Decision-makers are likely unable to quickly and easily determine the intent behind an intrusion. Other possible motivations for the intrusion include monitoring the target's military operations or gathering intelligence about its offensive cyber operations.³⁸ The specifics of the intrusion may provide some hints of intent but are unlikely to be definitive. For example, the target could use forensics to determine whether the intrusion took place during or just before the crisis, which could signal that an intruder intends to use it to influence the crisis. The ease with which the intrusion is discovered could also signal that the intruder intended to use it immediately and chose not to take the time to develop a stealthier presence. Testing of small-scale attacks or an uptick in communication between the intruder and code it has implanted in the target system could also signal that it is OPE.³⁹

The intruder would also have difficulty reassuring the target state of its intent because the Schelling-esque communication of commitment, priorities, and limits is fiendishly difficult for perpe-

36 The time required to prepare a network for offensive cyber operations may vary according to the vulnerability of the target. See, Long, "A Cyber SIOP?" 120–1; Borghard and Lonergan, "Cyber Operations as Imperfect Tools of Escalation," 125–131.

37 Lin, "Escalation Dynamics and Conflict Termination in Cyberspace."

38 Buchanan, *The Cybersecurity Dilemma*, chaps. 3 and 8.

39 Libicki, "Drawing Inferences from Cyber Espionage," 4–6.

trators of cyber operations.⁴⁰ To preserve its operational security, the intruder would have incentives not to acknowledge which adversary networks it has exploited and for what purpose, lest the target use that information to remove the intruder.⁴¹ Even if the intruder sought to reassure the target of its intent not to use the intrusion to enable an attack, it probably could not do so. A hack begun with one intent is able to shift purposes to serve another, undermining the credibility of such assurances.

The Inadvertent Escalation Pathway

The specific claim that cyber operations create incentives to use force in a crisis is an example of a more general claim that military operations and technology can cause misperceptions among adversaries with serious consequences for international conflict.⁴² One potential consequence of those misperceptions is inadvertent escalation, which occurs “when a combatant deliberately takes actions that it does not perceive to be escalatory but are interpreted that way by the enemy.”⁴³ The canonical scenario of inadvertent escalation is a conventional war among nuclear powers in which one party conducts “large-scale conventional operations that produce patterns of damage or threat to the major elements of a state’s nuclear force.”⁴⁴ The target state interprets the attack as a delib-

erate attempt to degrade its nuclear force and responds by using nuclear weapons or accelerating preparations for their use, although it could also ignore the effect of the attack on its nuclear arsenal.⁴⁵ Inadvertent nuclear escalation occurs as an unintended consequence of conventional military operations. Similarly, escalation to the use of cyber or kinetic force could occur in a crisis as an unintended consequence of the normal conduct of cyber espionage.

Scholars argue that misperceptions commonly associated with the security dilemma are one reason that inadvertent escalation could occur.⁴⁶ Specifically, the difficulty of distinguishing between an adversary’s offensive and defensive military operations is sufficient to produce misperceptions about the intent of the attacking state within the target state.⁴⁷ The attacking state’s conventional military operations could therefore make its adversary less secure in unintended ways,⁴⁸ which creates an incentive for the target state to use force sooner rather than later.⁴⁹

Similarly, the OPE-espionage distinction problem could trigger the use of force if the target state’s leaders make worst-case-scenario assessments of the attacker’s intent and capability to damage an important, compromised information network. The target state need only calculate that its ability to achieve its conflict objectives will diminish in the fu-

40 Thomas C. Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 1966), 47–48. For consideration of this point in cyber operations, see, Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* (Cambridge, MA: Harvard University Press, 2020); Jacquelyn G. Schneider, “Deterrence In and Through Cyberspace,” in *Cross-Domain Deterrence: Strategy in an Era of Complexity*, ed. Erik Gartzke and Jon R. Lindsay (New York, NY: Oxford University Press, 2019), 116–8; Valeriano, Jensen and Maness, *Cyber Strategy: The Evolving Character of Power and Coercion*.

41 For discussion of this principle and how information aids defense, see, Buchanan, *The Cybersecurity Dilemma*, chap. 3. See also, Erik Gartzke and Jon R. Lindsay, “Politics by Many Other Means: The Comparative Strategic Advantages of Operational Domains,” *Journal of Strategic Studies* (Published online, June 2020), 23–4, <https://doi.org/10.1080/01402390.2020.1768372>. For a skeptical view that offensive cyber capabilities would be lost if signaled to an adversary, see, Herb Lin, “U.S. Cyber Infiltration of the Russian Electric Grid: Implications for Deterrence,” *Lawfare*, June 18, 2019, <https://www.lawfareblog.com/us-cyber-infiltration-russian-electric-grid-implications-deterrence>.

42 Robert Jervis, “Cooperation Under the Security Dilemma,” *World Politics* 30, no. 2 (January 1978): 199–214, <https://www.jstor.org/stable/2009958>; Caitlin Talmadge, “Emerging Technology and Intra-War Escalation Risks: Evidence from the Cold War, Implications for Today,” *Journal of Strategic Studies* 42, no. 6 (2019): 864–87, <https://doi.org/10.1080/01402390.2019.1631811>.

43 Morgan et al., *Dangerous Thresholds*, xiii.

44 Barry R. Posen, *Inadvertent Escalation: Conventional War and Nuclear Risks* (Ithaca, NY: Cornell University Press, 1991), 3.

45 Posen, *Inadvertent Escalation*, 3–4. Inadvertent escalation could also occur in a purely conventional conflict. See, Talmadge, “Emerging Technology and Intra-War Escalation Risks,” 368.

46 Organizational factors and the fog of war provide alternative mechanisms linking the attacker’s actions to the target’s increased nuclear alert status or use. See, Posen, *Inadvertent Escalation*, 14–29.

47 States are likely to misperceive each other’s capabilities and actions as threatening, as the security dilemma claims, if it is either easier for states to conduct offensive operations than defensive operations (i.e., the offense-defense balance favors the offense), or impossible to distinguish between offensive and defensive capabilities or operations (i.e., offense and defense are indistinguishable). Jervis, “Cooperation Under the Security Dilemma,” 186–7. The offense-defense balance does not need to favor the offense for inadvertent escalation to occur, although it can intensify the victim state’s incentives to use force.

48 Posen, *Inadvertent Escalation*, 1–3.

49 This calculation is distinct from, but could be enhanced by, a first-mover advantage. Offense-defense theorists disagree on whether first-mover advantages should be included in the offense-defense balance. See, Jervis, “Cooperation Under the Security Dilemma,” 189; Charles L. Glaser and Chaim Kaufmann, “What Is the Offense-Defense Balance and How Can We Measure It?” *International Security* 22, no. 4 (April 1, 1998): 71–2, <https://doi.org/10.1162/isec.22.4.44>. Slayton defines the balance in cyberspace according to the relative cost and utility of attacking or defending a particular network, which could encompass a first-mover advantage. Rebecca Slayton, “What is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment,” *International Security* 41, no. 3 (2017): 72–109, https://doi.org/10.1162/ISEC_a_00267.

ture if it ignores the attacker's actions now.⁵⁰ There are four mechanisms by which a state could make a worst-case-scenario assessment of the seriousness of the threat posed by an intrusion and decide to use force: avoiding a military disadvantage, perceptions of an adversary's hostile intent, emotions, and information asymmetries within bureaucracies. The use of force, whether a cyber or kinetic attack, could serve a variety of purposes: to preempt an adversary's use of force in the crisis, to use a hacked military system before its functions are disrupted, to send a signal to the adversary to stop hacking the target's military systems, or to destroy or degrade the adversary's cyber forces that would otherwise carry out the attack on the target network.

Most obviously, a state that detects an adversary's OPE might use force to preempt a cyber attack that could put the state at a military disadvantage in a future conflict. Attacking immediately could preserve the state's confidence in its ability to operate its military forces as planned in the future.⁵¹ Given how quickly an attack can follow completed OPE, some decision-makers may consider any intrusion into an important network, such as a strategic military command-and-control network or a civilian network that supports military operations, to pose a serious threat. Weaker conventional military powers might lose vulnerable conventional or nuclear capabilities essential to staving off defeat.⁵² Stronger military powers might lose exquisite capabilities that enable a decisive victory but are less likely to succeed if information networks are degraded.⁵³ Decision-makers might ideally prefer to attribute the intrusion to its source and gather information about the possible intent behind the intrusion before making a decision to respond with force. They might also prefer to expel the intruder from the network and conduct a thorough decontamination effort. But both of those activities take time, which decision-makers do not have in a crisis. The combination of time pressure and the po-

tential for diminished military effectiveness gives decision-makers an incentive to use force earlier than they otherwise might in a crisis.⁵⁴

A second mechanism linking the discovery of an intrusion to the use of force concerns the effect of discovering the intrusion on the target's assessments of an adversary's intentions. States tend to assume the worst about their adversary's intentions when they cannot distinguish between the offensive or defensive nature of a weapon.⁵⁵ In addition, the adversary's actions — those that helped to produce the crisis — are likely to confirm the state's suspicions of its adversary's hostile intent.⁵⁶ These dynamics are likely to lead decision-makers to assume the worst about the intent behind the intrusion: They will assume that it is OPE and not merely espionage.⁵⁷ A state might even treat the discovery of an intrusion as an indicator that an adversary's conventional attack is imminent.⁵⁸ The combination of the crisis environment and OPE-espionage distinction problem could lead the state to attribute aggressive intentions to the adversary with regards to both the network intrusion and the overall crisis, incentivizing the use of force rather than the pursuit of a diplomatic resolution.

A third mechanism concerns decision-makers' emotions. Rose McDermott argues that cyber operations are likely to trigger emotions of fear, anger, and surprise, all of which affect an individual's levels of optimism and risk-acceptance in their reactions. In addition, "individuals differ systematically in their basic trait levels of fear and anger."⁵⁹ Fear is likely to lead to more pessimism and risk-avoidance in responses, which could prompt an individual to negotiate an end to a confrontation following a cyber attack. Anger is likely to lead to more optimistic and risk-seeking behavior, which is more likely to lead to retaliation. If decision-makers are surprised by cyber attacks, they are more likely to hold others responsible for their effects. Surprised individuals might be more likely to judge cyber operations as

50 This could involve a state facing pressure to either "use or lose" its weapons or signal resolve in case its adversary's conflict objectives expand in future. See, Jervis, "Cooperation Under the Security Dilemma," 189; Schelling, *Arms and Influence*, chap. 6; Talmadge, "Would China Go Nuclear?" 57.

51 Posen, *Inadvertent Escalation*, 2.

52 Posen, *Inadvertent Escalation*, 2.

53 Acton, "Escalation Through Entanglement," 73–76. In the context of nuclear operations, Acton refers to this inadvertent escalation pathway as a damage limitation window of opportunity.

54 For a discussion of military information network use-or-lose dynamics, see, Talmadge, "Emerging Technology and Intra-War Escalation Risks," 880.

55 Jervis, "Cooperation Under the Security Dilemma," 199.

56 For a similar argument about the impact of the onset of conflict on a state's perceptions of its adversary's military actions and intentions, see, Talmadge, "Would China Go Nuclear?" 62–3.

57 Robert Jervis, *Perception and Misperception in International Politics* (Princeton, NJ: Princeton University Press, 1976), 67–72.

58 Acton, "Escalation Through Entanglement," 67–73. In the context of nuclear operations, Acton refers to this inadvertent escalation pathway as misinterpreted warning.

59 Rose McDermott, "Some Emotional Considerations in Cyber Conflict," *Journal of Cyber Policy* 4, no. 3 (2019): 316, <https://doi.org/10.1080/23738871.2019.1701692>.



deliberate rather than accidental.⁶⁰ These insights suggest that if decision-makers react to the surprise of discovering an intrusion with anger, they might be more likely to escalate to the use of force than continue to negotiate a resolution to the crisis.

A final mechanism concerns the uneven distribution of information about the nature of cyber operations in national security bureaucracies. Intrusions that some cyber specialists see as a routine part of cyber operations may alarm more senior generalists, especially in a crisis. Top decision-makers may not have sufficient knowledge or information to assess the risks posed by a cyber intrusion to their military capabilities.⁶¹ Decision-makers generally have a hard time interpreting the nuances of cyber operations because they may not have a good understanding of those operations or may understand them through analogies that do not capture the complexity of cyber OPE. For example, Deputy Secretary of Defense Robert Work once described fairly low-level operations against the Islamic State as “dropping cyberbombs.”⁶² Members of the bureaucracy who are more familiar with the routine part of cyber operations, such as the operators responsible for securing military networks, might not be in the situation room in a crisis to help decision-makers accurately assess the seriousness of the intrusion.

The Deliberate Escalation Pathway

These four mechanisms explain how inadvertent escalation from an intrusion believed to be OPE could result in the use of force. However, scholars have questioned whether states make decisions to escalate because of the independent effects of technology alone. Based on historical case studies, Caitlin Talmadge argues that new technologies might not force decision-makers to take escalatory actions, but rather “seem likely to be an intervening variable.” The technological characteristics of weapons that create risks of escalation “could en-

able or accelerate escalatory pressures originating elsewhere, particularly in state policies or military doctrines that intentionally seek to manipulate escalatory risk.” In other words, states seek out new technologies to enable them to increase risk of escalation, or turn to them opportunistically in a conflict, rather than their hands being forced to escalate in a crisis because they did not anticipate the escalatory pressures that their prior decisions to deploy certain military capabilities would create.⁶³ These actions constitute deliberate escalation: “[when] a combatant deliberately increases the intensity or scope of an operation to gain an advantage or avoid defeat.”⁶⁴

The deliberate escalation hypothesis suggests that states might assess that a cyber intrusion poses a serious but tolerable threat, yet choose to use force in response because they have strategic and political incentives to escalate. Those strategic and political incentives usually involve gaining a military advantage, signaling resolve, or preempting an adversary’s attempt to signal resolve by using force.⁶⁵ A deliberate escalation pathway is unlikely to involve emotional or organizational mechanisms, but is likely to involve military disadvantage and misperception mechanisms.

The Bluster De-Escalation Pathway

Decision-makers may decide not to use force if they discover an intrusion in a crisis — even if they are confident that the intruder has performed OPE — because they do not think the intrusion poses a serious threat. This hypothesis draws on existing empirical research, which indicates that cyber attacks are perceived to be more bluster than bite. States and individuals tend not to retaliate in response to cyber attacks.⁶⁶ One explanation for this empirical finding is that decision-makers do not view cyber attacks as sufficiently damaging or destructive to warrant the use of force in response.⁶⁷

60 McDermott, “Some Emotional Considerations in Cyber Conflict,” 318–323.

61 Scholars of inadvertent escalation point to similar organizational dynamics within an attacking state. Military planners often do not involve civilians in operational planning and are slow to transmit information about ongoing operations to leaders. See, Posen, *Inadvertent Escalation*, 16–19.

62 David Sanger, “U.S. Cyberattacks Target ISIS in a New Line of Combat,” *New York Times*, April 24, 2016, <https://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html>.

63 Talmadge, “Emerging Technology and Intra-War Escalation Risks,” 890, 868–9.

64 Morgan et al., *Dangerous Thresholds*, xii.

65 Goldstein, “First Things First,” 75–77.

66 See for example, Kreps and Schneider, “Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains”; Schneider, “The Information Revolution and International Stability”; Benjamin Jensen and Brandon Valeriano, *What Do We Know About Cyber Escalation? Observations From Simulations and Surveys* (Washington, DC: Atlantic Council, November 2019); Valeriano and Maness, *Cyber War Versus Cyber Realities*; Jensen, Valeriano, and Maness, *Cyber Strategy: The Evolving Character of Power and Coercion*.

67 Jensen, Valeriano, and Maness, *Cyber Strategy: The Evolving Character of Power and Coercion*; Borghard and Loneran, “Cyber Operations as Imperfect Tools of Escalation,” 131–3; Borghard and Loneran, “The Logic of Coercion in Cyberspace,” 466–71; Gartzke, “The Myth of Cyberwar”; Lindsay, “Stuxnet and the Limits of Cyber Warfare”; Gartzke and Lindsay, “Politics by Many Other Means,” 21–4.

Applying these arguments to a crisis scenario in which an intrusion is discovered, decision-makers might calculate that the cost of the cyber attack is likely to be low and can be absorbed. This explanation suggests that states would not anticipate a military disadvantage from a cyber attack — the opposite outcome of the military disadvantage mechanism outlined above.

Decision-makers might even view cyber attacks as a signal that an adversary intended to avoid a conventional conflict. When the effects of cyber and kinetic attacks are held constant, U.S. survey respondents were less likely to support retaliation for cyber attacks than kinetic attacks.⁶⁸ Decision-makers might therefore interpret the discovery of an intrusion as a signal of an adversary's intent to avoid crossing the threshold of conventional armed conflict,⁶⁹ rather than its hostile intent — the opposite outcome of the misperception mechanism outlined above. A final reason decision-makers could assess that a cyber intrusion does not pose a serious threat is that they are confident that the threat of in-kind or cross-domain retaliation will deter the adversary from actually carrying out large-scale cyber attacks enabled by the intrusion.⁷⁰

The Countervailing De-Escalation Hypothesis

Finally, decision-makers might view the intrusion as posing a serious threat but have countervailing political or strategic incentives not to respond with the use of force. Decision-makers could react to an intrusion in this de-escalatory manner if they want to defuse the crisis for political or strategic reasons. States are likely to find themselves in this situation if the stakes of the crisis do not merit fighting a war, or if the state could not achieve its political objectives with conventional military operations. Decision-makers with multiple adversaries might also be wary of misattributing an intrusion carried out by one adversary to another if they cannot attribute the intrusion to its perpetrator with sufficient confidence in the time frame of the crisis.⁷¹ Other countervailing incentives may also originate in domestic politics. The ambiguity of intent behind cyber intrusions could help moderate decision-makers build a coalition for restraint in the crisis and counter the policy prefer-

ences of more hawkish decision-makers.⁷² Any of the four mechanisms leading to inadvertent escalation might apply in this pathway, but their effect on the use of force would be extinguished by countervailing incentives.

Evaluating Cyber Escalation Hypotheses

How might scholars determine which of these four hypotheses is most likely in a great-power crisis? No political crisis has occurred between the United States and China (or Russia) since those countries acquired cyber capabilities in the mid-2000s. No research design offers a perfect solution to the problem of assessing claims about events that have not occurred. To complement existing empirical studies involving U.S. participants, our approach focuses on capturing differences between U.S. and Chinese approaches to cyber conflict. Our empirical analysis in the next three sections is guided by the following observable implications of the four hypotheses outlined above.

The inadvertent escalation hypothesis would expect states to express concern about any intrusions into their networks and to recognize the OPE-espionage distinction problem. States might also recognize inadvertent escalation risks and take steps to manage cyber escalation risks in their procedures, authorities, and cyber operations organizational structures. Inadvertent escalation is also more likely to occur when two states have a poor understanding of each other's cyber activities and lack crisis communications mechanisms to verify the nature of an intrusion. A lack of recognition of inadvertent escalation risks could support either the inadvertent escalation hypothesis or the bluster de-escalation hypothesis. A state that possesses good attribution capabilities, defends its network against intrusions, and effectively repels intruders who do breach defenses might be less likely to experience worrying intrusions. States possessing those capabilities might also be able to better assess the intent and the severity of the threat posed by an intrusion. Those capabilities are more likely to support the bluster de-escalation hypothesis.

While it is difficult to describe the strategic and political incentives that could provide evidence to support the deliberate escalation or countervailing

68 Kreps and Schneider, "Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains."

69 Austin Carson, *Secret Wars: Covert Conflict in International Politics* (Princeton, NJ: Princeton University Press, 2018), 296.

70 Scholars debate the effectiveness of efforts to deter cyber attacks with threats of in-kind or cross-domain retaliation. See, Nye, "Deterrence and Dissuasion in Cyberspace"; Schneider, "Deterrence In and Through Cyberspace," 112–5.

71 Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no. 1–2 (2015): 32, <https://doi.org/10.1080/01402390.2014.977382>.

72 Carson, *Secret Wars*, 296.

hypotheses in a future crisis, some *ex ante* features of a great-power relationship would shape those incentives. Deliberate escalation is more likely to occur when the state discovering the intrusion is conventionally stronger than its adversary, does not confront multiple nation-state adversaries in cyberspace, or has high political stakes in the crisis. The countervailing hypothesis is more likely to find support if the state discovering the intrusion is conventionally weaker than its adversary, faces multiple nation-state adversaries in cyberspace, or has low political stakes in the crisis. Reflecting our intent to examine the most likely case for inadvertent escalation resulting from cyber operations, a crisis scenario between the United States and China is less likely to support the countervailing de-escalation hypothesis than other dyads. The conventional military balance between these two states is becoming more equal.⁷³ The independent effect of cyber technology on Chinese incentives to use force is therefore less likely to be obfuscated by strategic disincentives to use force.

Escalation Risks in U.S. Cyber Operations

Evidence from the United States indicates that the country's decision-makers recognize the inadvertent escalation risks posed by cyber operations and OPE in particular. But U.S. decision-makers have taken steps to mitigate those risks. The Obama administration implemented organizational practices that carefully managed cyber operations that could produce escalation. The Trump administration relaxed those organizational practices after gaining confidence in operational practices, such as persistent defenses, a policy of more actively thwarting would-be intruders, and good attribution capabilities. In this manner, evidence from the United States supports both the inadvertent escalation hypothesis and the bluster de-escalation hypothesis. As part of its more aggressive approach, U.S. Cyber Command has also concluded that most cyber intrusions could not produce serious enough effects to result in escalation. This judgment could support the blus-

ter de-escalation hypothesis and the countervailing de-escalation hypothesis. U.S. adversaries might view its intrusions as very threatening but face strategic and political incentives not to use force, especially given their conventional military inferiority to the United States.

Leadership Views of OPE

The public statements of U.S. leaders and U.S. government reactions to discoveries of intrusions into military networks indicate that the United States views intrusions as threatening, in part because they could be used either for OPE or intelligence gathering. At the worldwide threat briefing each year since 2010, the director of national intelligence has placed the risk of foreign hacking as the top national security threat facing the United States.⁷⁴ After a Russian hack of Pentagon systems in 2015 that the United States was able to repel, then-Secretary of Defense Ash Carter summarized the American position aptly when he said, "[It] can't be good for anybody to be inside of our networks — whatever their motivation."⁷⁵ Similarly, Gen. Paul Nakasone, the head of the National Security Agency (NSA) and U.S. Cyber Command, wrote in an essay with his adviser Michael Sulmeyer that the United States turned to a more aggressive policy "to prevent footholds from turning into beachheads so that a single compromise will not threaten the military's ability to accomplish its mission."⁷⁶ The clarity of this expressed vision — strongly pushing back against any kind of foreign hacking of crucial systems — is remarkable and indicative of current U.S. policy.

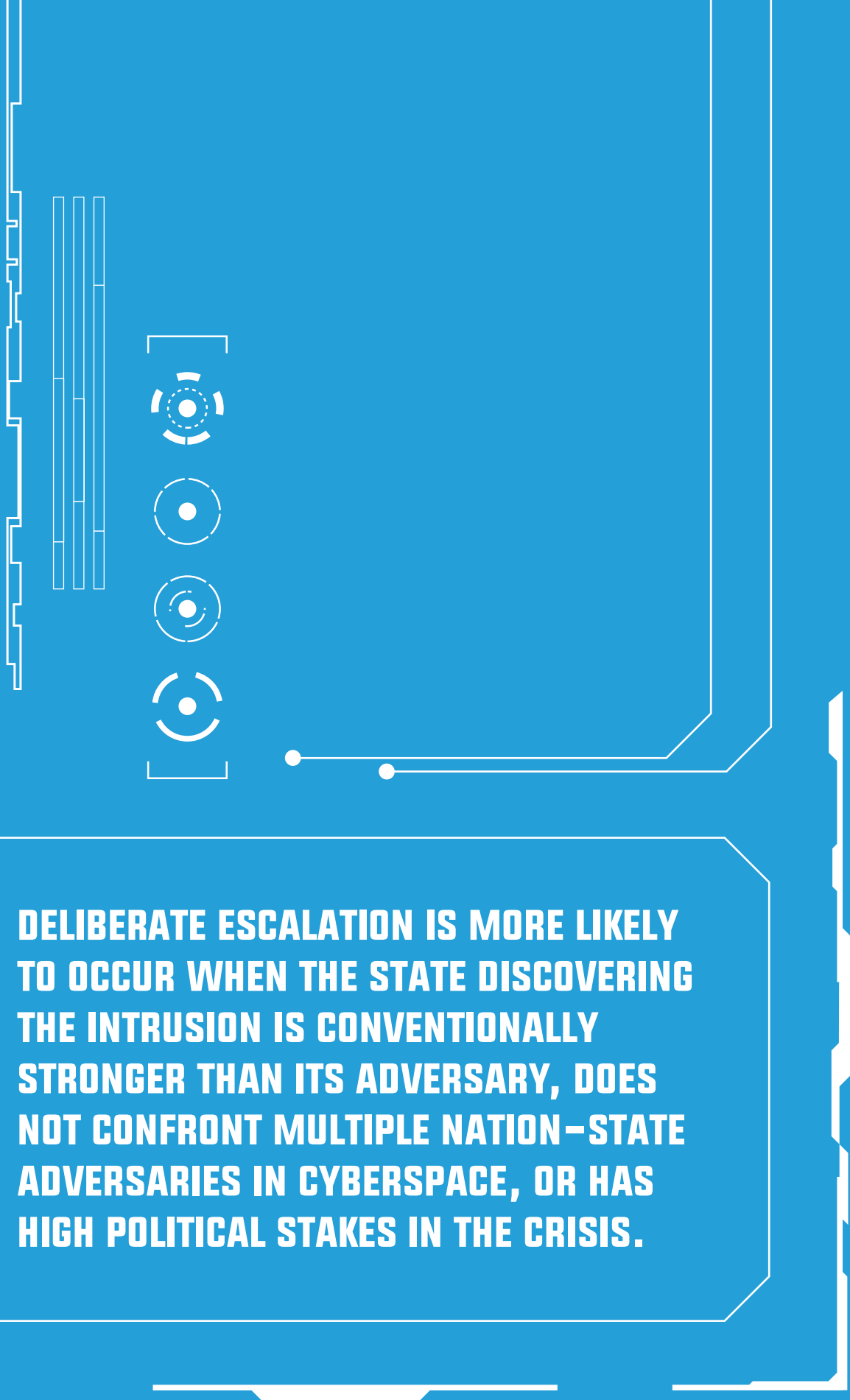
While most U.S. responses to foreign hacking efforts are highly classified, two historical cases show how U.S. policymakers worried about the implications of minor intrusions. In a 1998 hack known as Solar Sunrise, intruders penetrated the U.S. military's logistics and communications networks. The Joint Staff general in charge of information operations, John Campbell, worried that the breach would permit significant attacks, especially at a time of heightened tensions with Iraq. "If you take one part of that machine, and disable it," he said, "you[ve] got a real problem trying to make a deployment take

73 Eric Heginbotham, Michael Nixon, Forrest E. Morgan, Jacob L. Heim, Sheng Tao Li, Jeffrey Engstrom, Martin C. Libicki, Paul DeLuca, David A. Shlapak, David R. Frelinger, Burgess Laird, Kyle Brady, and Lyle J. Morris, *The U.S.-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power, 1996-2017* (Santa Monica, CA: RAND Corporation, 2015).

74 For example, Daniel R. Coats, "Worldwide Threat Assessment of the United States Intelligence Community," Senate Select Committee on Intelligence, Jan. 29, 2019, <https://www.odni.gov/index.php/newsroom/congressional-testimonies/item/1947-statement-for-the-record-worldwide-threat-assessment-of-the-us-intelligence-community>.

75 Shane Smith, "Cyberspies, Nukes, and the New Cold War: Shane Smith Interviews Ashton Carter (Part 1)," *Vice*, May 15, 2015, 2:13, <https://www.vice.com/en/article/xw3b4n/cyberspies-nukes-and-the-new-cold-war-shane-smith-interviews-ashton-carter-part-1>.

76 Paul M. Nakasone and Michael Sulmeyer, "How to Compete in Cyberspace," *Foreign Affairs*, Aug. 25, 2020, <https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity>.



DELIBERATE ESCALATION IS MORE LIKELY TO OCCUR WHEN THE STATE DISCOVERING THE INTRUSION IS CONVENTIONALLY STRONGER THAN ITS ADVERSARY, DOES NOT CONFRONT MULTIPLE NATION-STATE ADVERSARIES IN CYBERSPACE, OR HAS HIGH POLITICAL STAKES IN THE CRISIS.



place.”⁷⁷ Campbell’s comments reflect an assessment that the intrusion could have placed the United States at a military disadvantage in a conflict. The discovery did not take place during a major crisis and therefore lacked the time pressure element that would create incentives to use force. Nevertheless, it was only after various parts of the U.S. government spun up to prepare for a response that an investigation concluded the breach was the work of three teenagers and their 20-year-old mentor. In short, because of OPE’s dangers, even hacks carried out for kicks and bragging rights caused major alarm in the U.S. government.

In another case, *Moonlight Maze*, U.S. policymakers responded with great alarm. The attack occurred in 1998 and 1999 and involved Russian penetration of unclassified American networks. The U.S. government hacked back into Russian computers in order to gain more intelligence.⁷⁸ One of the White House’s top national security officials, Richard Clarke, labeled the activities “cyberwar reconnaissance.”⁷⁹ Then-Deputy Secretary of Defense John Hamre went still further, telling the Intelligence Committees of Congress in a classified briefing that the United States was “in the middle of a cyber war.”⁸⁰ These comments indicate once more that U.S. decision-makers view intelligence collection as enabling the use of force in cyberspace.

OPE in Cyber Operations

U.S. operators and decision-makers have recognized the need for OPE to conduct sophisticated cyber operations since at least 2010. The vice chairman of the Joint Chiefs of Staff issued a memo in 2010 mandating the use of the term “Cyber Operations in Preparation of the Environment,” which referred to those cyber operations that serve “as an enabling function for another military operation.” This updated a 2005 instruction that was more vague but nonetheless referred to the need to shape the digital environment in order to aid operations.⁸¹

From the earliest days of the U.S. Cyber Command, secret documents — now declassified — indicated that conducting OPE was one of its core tasks.⁸²

Planners at the highest levels of the U.S. government eventually recognized the importance of OPE. During the Obama administration, the most significant high-level document governing America’s offensive cyber capability was *Presidential Policy Directive 20* (PPD-20). The president signed the classified document in secret in the fall of 2012, but the White House released a fact sheet that provided a limited level of detail. In the fact sheet, the White House made no mention of offensive cyber capabilities. Instead, it stated that the new policy “enables us to be flexible” and emphasized the White House plans on “exercising restraint.” The United States “shall undertake the least action necessary to mitigate threats” and “will prioritize network defense and law enforcement as preferred courses of action.”⁸³ In short, the unclassified readout of PPD-20 suggests a posture that pays little attention to either offensive action or to the preparation required to enable it.

But the full classified document, leaked in 2013 by Edward Snowden, reveals a strategy that directly considers offensive action and contrasts it with other forms of cyber operations. The strategy defines a clear typology of cyber activity. This includes “cyber collection,” which refers to intelligence-gathering activities for purposes other than offensive preparation. It also includes “non-intrusive defensive countermeasures,” meaning steps taken within one’s own network, such as deploying antivirus and other basic security measures. PPD-20 refers to other authorities and plans that govern both sets of activities. The document also introduces the concept of “Defensive Cyber Effects Operations.” It defines these activities as efforts that have an effect on an adversary’s computer systems — presumably, hacking or other interference — but only for the purposes of defense. For example, one could imagine a basic scenario in which an adversary is launching a cyber operation against American targets, and the

77 Thomas Rid, *Rise of the Machines: A Cybernetic History* (New York, NY: W. W. Norton & Company, 2016), 315.

78 Rid, *Rise of the Machines*, 327.

79 Rid, *Rise of the Machines*, 336.

80 “We’re in the Middle of a Cyberwar,” *Newsweek*, Sept. 19, 1999, <https://www.newsweek.com/were-middle-cyberwar-166196>. See also, Rid, *Rise of the Machines*, 338.

81 The earlier instruction said, “[The Defense Department] will use [computer] network exploitation to gather intelligence and shape the cyber-space environment as necessary to provide integrated offensive and defensive options.” See, Chairman of the Joint Chiefs of Staff, *The National Military Strategy for Cyberspace Operations*, 2006, 2, <https://www.hsdl.org/?abstract&did=35693>. For the later instruction, see, Vice Chairman of the Joint Chiefs of Staff, “Memorandum: Subject: Joint Terminology for Cyberspace Operations,” 2010, 7, <http://www.nsci-va.org/CyberReferenceLib/2010-11-Joint%20Terminology%20for%20Cyberspace%20Operations.pdf>.

82 U.S. Strategic Command, “CYBERCOM Announcement Message,” May 21, 2010, 2, from “The United States and Cyberspace: Military Organization, Policies, and Activities,” *National Security Archive*, Jan. 20, 2016, <https://nsarchive.gwu.edu/briefing-book/cyber-vault/2016-01-20/united-states-cyberspace-military-organization-policies-activities>.

83 “Fact Sheet on Presidential Policy Directive 20,” The White House, Federation of American Scientists, 2012, <https://fas.org/irp/offdocs/ppd/ppd-20-fs.pdf>.

United States conducts a basic cyber attack to interfere with the adversary's internet connectivity and inhibit the adversary's action. PPD-20 provides high-level procedures for managing this kind of aggressive defensive action.⁸⁴

Most significantly, though, the classified version of PPD-20 defines offensive action in more detail than the declassified fact sheet. It introduces the concept of "Offensive Cyber Effects Operations" (OCEO). This is the class of activities that are not cyber collection, non-intrusive defensive countermeasures, or defensive cyber effects operations. Instead, these efforts are designed to cause effects in adversary networks.⁸⁵ The document extols the unique virtues of these kinds of offensive cyber operations, which "can offer unique and unconventional capabilities to advance U.S. national objectives around the world with little or no warning to the adversary or target and with potential effects ranging from subtle to severely damaging."⁸⁶

PPD-20 acknowledges the need for OPE to bring these offensive options to fruition. The document's authors explicitly recognize the preparation needed to develop such capabilities: "The development and sustainment of [offensive cyber] capabilities, however, may require considerable time and effort if access and tools for a specific target do not already exist."⁸⁷ PPD-20 directs the U.S. government to begin this operational preparation. The relevant agencies "shall identify potential targets of national importance where OCEO can offer a favorable balance of effectiveness and risk as compared with other instruments of national power, [and] establish and maintain OCEO capabilities integrated as appropriate with other U.S. offensive capabilities."⁸⁸ In so doing, PPD-20's authors reveal that they understand what is required to enable offensive capabilities and that they believe the United States should — in secret — take those steps. With his signature, President Barack Obama authorized the preparatory activity.

Procedures for Managing Escalation Risks

PPD-20 reveals U.S. policymakers' cognizance of the risks that arise from actually *using* offensive cyber capabilities. As a result, as much as it discusses and authorizes preparation of the en-

vironment, the document highlights a process to carefully manage offensive actions that might do serious harm or invite escalation. The document emphasizes interagency coordination, balancing defense and national security interests with diplomatic and economic ones. Most notably, the process requires the highest level of executive branch oversight — presidential approval — for any cyber operation that is "reasonably likely to result in significant consequences."⁸⁹ This term is broadly defined: "Loss of life, significant responsive actions against the United States, significant damage to property, serious adverse U.S. foreign policy consequences, or serious economic impact on the United States."⁹⁰ It is likely that cyber operations that do not meet that threshold could otherwise be approved by the agency carrying out the operation without such high-level interagency vetting.

Crucially, PPD-20 does not limit these restrictions to cyber attacks, but emphasizes that they apply to all cyber operations. In short, Obama wanted direct oversight of any operation that might meet the threshold of significant consequences — regardless of whether that operation involved collecting intelligence, defending American computers, preparing an offensive capability, or launching an attack. While it is impossible to know how agencies interpreted this directive, there seems to be little doubt that the Obama administration was concerned, at least in theory, about the risks of cyber escalation even as it appreciated the operational necessity to prepare offensive capabilities in advance.

The Trump administration has adopted a more relaxed set of organizational procedures for managing cyber escalation risks. Upon unveiling its new national cyber strategy in 2018, the Trump White House specifically chastised the preceding administration for what it saw as its overly cautious posture and promised to be more aggressive in its engagements with adversaries. Then-National Security Adviser John Bolton said, "Our hands are not tied as they were in the Obama administration." Other White House and Defense Department officials supported the same theme: It was time to take the gloves off. Nor was the need for more aggressive action just a partisan view. In his confirmation hearing, the incoming NSA director and commander of U.S.

84 Barack Obama, "Presidential Policy Directive/PPD-20, Subject: U.S. Cyber Operations Policy," Oct. 16, 2012, 2–3, from *National Security Archive*, <https://nsarchive2.gwu.edu/dc.html?doc=2725521-Document-2-9>.

85 Obama, "Presidential Policy Directive/PPD-20," 2–3.

86 Obama, "Presidential Policy Directive/PPD-20," 9.

87 Obama, "Presidential Policy Directive/PPD-20," 9.

88 Obama, "Presidential Policy Directive/PPD-20," 9.

89 Obama, "Presidential Policy Directive/PPD-20," 9.

90 Obama, "Presidential Policy Directive/PPD-20," 3.

Cyber Command Gen. Paul Nakasone warned that the United States had to do more because American adversaries “don’t fear us.”⁹¹

To translate this rhetoric into policy, President Donald Trump signed “National Security Presidential Memorandum 13.” The goal of the memorandum, which remains classified, is to provide military commanders greater flexibility to integrate cyber operations into their overall approach to warfighting and deterrence.⁹² By delegating this authority to the Pentagon, the Trump administration attempted to foster a faster and more aggressive process, one that will generate more operational effects more quickly. But this approach also rebalanced the trade-off between operational agility and whole-of-government coordination to manage cyber escalation risks in favor of the former. According to the general on the Joint Staff responsible for cyber operations, this change marked a notable contrast to the Obama administration’s approach, which was “an interagency process that went through the National Security Council ... to deputies’ committee to principals’ committee and [where], in effect, anyone could stop the process along the way.” Nor, he argued, was the distinction just semantics or bureaucratic minutia, but one that “makes all the difference in the world in terms of the speed at which you can move.”⁹³

Unlike PPD-20, the Trump memo has not leaked. It is impossible to know whether this new policy frees commanders to both launch cyber capabilities and prepare to do so. But there are hints that the memo and complementary legislative changes implemented by Congress provide a freer hand in developing the malicious code and gaining access to target networks required to provide commanders with offensive options. For example, in a recent media interview, the former deputy commander

of U.S. Cyber Command, Lt. Gen. Vincent Stewart, indicated that changes to congressional legislation “freed us up to do some of the things, the operational preparation of the environment, that we were limited from doing outside of the counterterrorism mission and now can do much more broadly against all of our peers and competitors.”⁹⁴ In addition, a *New York Times* story from June 2019 describes more aggressive American preparatory measures against the Russian power grid.⁹⁵

Overall, the Trump administration seems much less worried about the escalation risk associated with cyber operations than the Obama administration. Michael Daniel, the former coordinator for cyber security in the Obama White House, observed that the Trump administration “is willing to take more risks than previous administrations, but the proof will be in the results.”⁹⁶ While the administration’s approach remains untested in a crisis with a near-peer competitor, it has been informed by the U.S. experience with cyber conflict over the past decade as well as the increasing risk tolerance of U.S. decision-makers. To justify its new posture, U.S. Cyber Command has argued that “adversaries continuously operate against us below the threshold of armed conflict,” in what it described as a “new normal.”⁹⁷ Moreover, the command argued that U.S. efforts to counter this adversarial activity will not lead to retaliation in or outside of cyberspace that would cross that threshold.

These claims have been fiercely debated in the academic literature, with critics of the so-called persistent engagement approach arguing that the new strategy could produce escalation. For example, some contend that the thresholds for armed conflict are not as clear as U.S. Cyber Command has suggested. Others argue that persistent engagement creates too many red lines for adver-

91 David E. Sanger, “Trump Loosens Secretive Restraints on Ordering Cyberattacks,” *New York Times*, Sept. 20, 2018, <https://www.nytimes.com/2018/09/20/us/politics/trump-cyberattacks-orders.html>.

92 Mark Pomerleau, “New Cyber Authority Could Make ‘All the Difference in the World,’” *Fifth Domain*, Sept. 17, 2018, <https://www.fifthdomain.com/dod/cybercom/2018/09/17/new-cyber-authority-could-make-all-the-difference-in-the-world/>.

93 Pomerleau, “New Cyber Authority Could Make ‘All the Difference in the World,’” Sydney Freedberg, “Trump Eases Cyber Ops, but Safeguards Remain: Joint Staff,” *Breaking Defense*, Sept. 17, 2018, <https://breakingdefense.com/2018/09/trump-eases-cyber-ops-but-safeguards-remain-joint-staff/>.

94 Mark Pomerleau, “Is Cyber Command Really Being More ‘Aggressive’ in Cyberspace?” *Fifth Domain*, April 25, 2019, quoted in Jason Healey, “The Implications of Persistent (and Permanent) Engagement in Cyberspace,” *Journal of Cybersecurity* 5, no. 1 (2019): 3, <https://doi.org/10.1093/cybsec/tyz008>.

95 David E. Sanger and Nicole Perlroth, “U.S. Escalates Online Attacks on Russia’s Power Grid,” *New York Times*, June 15, 2019, <https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html>.

96 Nakashima, “White House Authorizes ‘Offensive Cyber Operations’ to Deter Foreign Adversaries,” *Washington Post*, Sept. 20, 2018, https://www.washingtonpost.com/world/national-security/trump-authorizes-offensive-cyber-operations-to-deter-foreign-adversaries-bolton-says/2018/09/20/b5880578-bd0b-11e8-b7d2-0773aa1e33da_story.html.

97 U.S. Cyber Command, *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command*, March 2018, 3, <https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010>.

saries and is therefore not a realistic means for shaping behavior.⁹⁸ Engaging with this debate, Nakasone and Sulmeyer wrote:

The thinking goes that by competing more proactively in cyberspace, the risk of miscalculation, error, or accident increases and could escalate to a crisis. Cyber Command takes these concerns seriously, and reducing this risk is a critical part of the planning process. We are confident that this more proactive approach enables Cyber Command to conduct operations that impose costs while responsibly managing escalation.⁹⁹

Capabilities for Managing Escalation Risks

In the past decade, the United States has developed some of the world's most sophisticated cyber capabilities to better defend its networks, attribute intrusions, and expel intruders in peacetime. To better defend networks, the United States has invested in major systems, such as EINSTEIN 3, that aim to thwart intrusions. To improve rapid attribution of intrusions and increase situational awareness, the United States established various cross-agency working groups and bulked up teams within the NSA and U.S. Cyber Command. To the extent that these capabilities work — which is hard to judge — they mitigate cyber escalation risks by reducing the likelihood that intruders will successfully break into U.S. networks and alarm policymakers who have to decide on how to respond within the compressed time period of a crisis.

Escalation Risks in Chinese Cyber Operation

The sources providing evidence of China's approach to cyber operations are older, scarcer, and less authoritative than those for the United States. Nevertheless, they still offer valuable insights for policy and scholarly debates about cyber conflict, which rarely draw on Chinese empirics. These sources suggest that China is much less cognizant of the inadvertent escalation risks posed by OPE than the United States. Indeed, there is little evidence that China has scrutinized these risks as carefully

as the United States. This lack of attention could be evidence of the bluster de-escalation hypothesis, as it might reflect a judgment that inadvertent escalation risks are manageable. But it is more likely that there is a lack of awareness of these inadvertent escalation risks in China. In addition, China will also face weaker countervailing strategic incentives not to use force in response to cyber intrusions in the future compared with the past, as it continues to chip away at the decisive U.S. conventional military advantage in the Indo-Pacific.

China's apparent lack of awareness of the inadvertent escalation risks associated with OPE could help to realize such risks in a crisis for three reasons. First, China is more likely to misperceive U.S. cyber intrusions. Second, it is more likely to overlook the ways that its own cyber intrusions could be misperceived. Third, China is much less likely to take steps to mitigate these risks. Available sources provide no evidence that the People's Liberation Army (PLA) has practices to manage inadvertent escalation. However, China is investing in cyber situational awareness to improve its network defenses and attribution capabilities. These measures could mitigate cyber escalation risks in the future, even if they are not pursued with this purpose in mind.

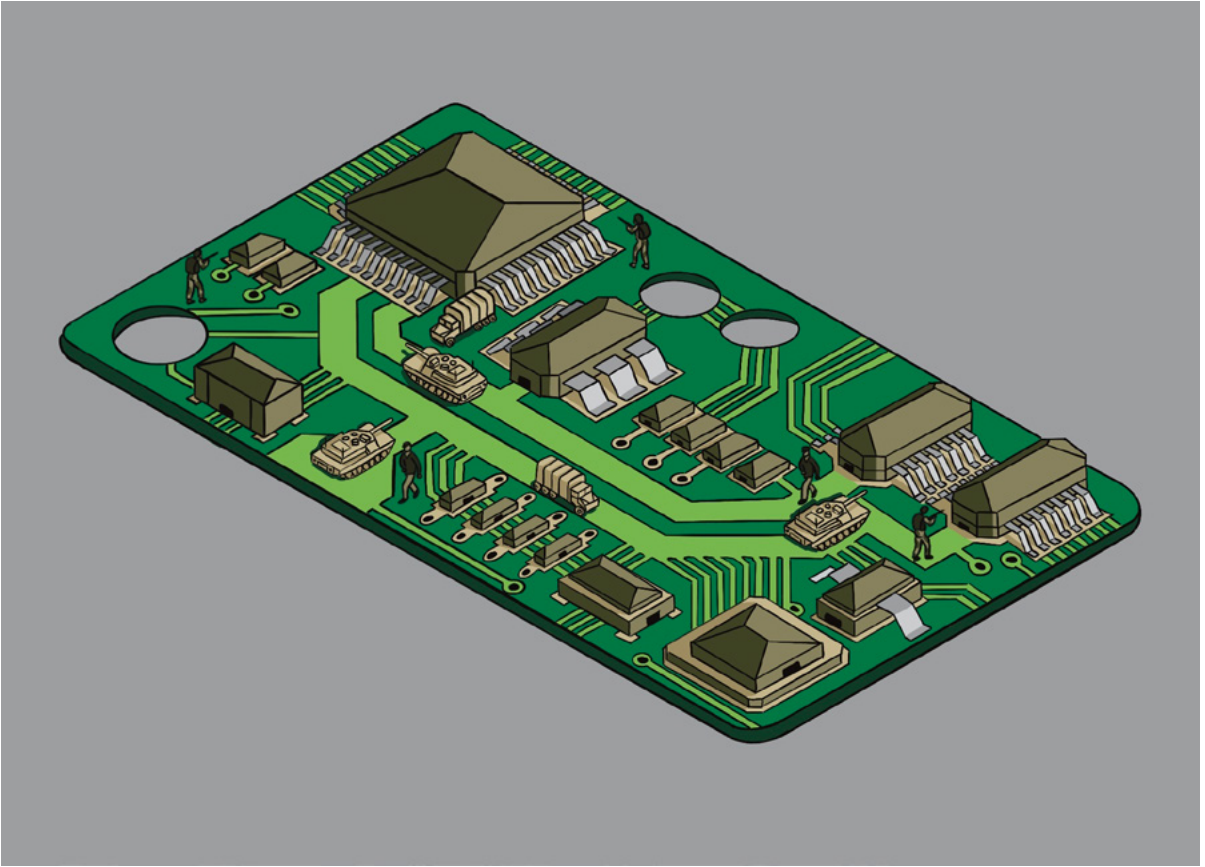
The Chinese government does not officially acknowledge that the PLA has an offensive cyber operations capability. The authoritativeness, completeness, and availability of sources with which to assess China's views of cyber escalation risks are more limited as a result. But China's offensive cyber capabilities are acknowledged in the teaching, research, and strategy publications of influential PLA organizations such as the Academy of Military Science and National Defense University. The PLA's official newspaper and cyber security publications associated with civilian bodies also discuss offensive cyber capabilities. This article examines those sources, in accordance with the best practices for open-source research on Chinese military strategy.

Leadership Views of OPE

Chinese policymakers' fears about foreign hackers have grown in tandem with the expansion of the Chinese government and military's dependence on computer networks. In a major speech on national cyber security policy in 2016, Communist Party Gen-

98 For arguments in favor of persistent engagement, see, Michael P. Fischerkeller and Richard J. Harknett, *Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics, and Escalation* (Washington, DC: Institute for Defense Analyses, May 2018); Richard J. Harknett and Michael P. Fischerkeller, "What Is Agreed Competition in Cyberspace?" *Lawfare*, Feb. 19, 2019, <https://www.lawfareblog.com/what-agreed-competition-cyberspace>. For critiques, see, Healey, "The Implications of Persistent (and Permanent) Engagement in Cyberspace"; Max Smeets, "There Are Too Many Red Lines in Cyberspace," *Lawfare*, March 20, 2019, <https://www.lawfareblog.com/there-are-too-many-red-lines-cyberspace>. See also, Aaron Brantly, ed., *The Cyber Deterrence Problem* (New York, NY: Rowman & Littlefield, 2020).

99 Nakasone and Sulmeyer, "How to Compete in Cyberspace."



eral Secretary Xi Jinping stated that, “Cyber security has a strong covert character; a technological vulnerability or security risk can stay hidden for a number of years without being discovered.” As a result, “we do not know who came in, whether it was an enemy or a friend, or what they did.” Xi implied that while this enemy or friend’s intrusion could remain “latent” inside a network for a long time, it could be “activated whenever (*yidan jiu fazuo le*).”¹⁰⁰

The Chinese government has not publicly acknowledged any specific incidents in which it discovered that foreign state actors had exploited its government or military networks. The closest analogue to the Solar Sunrise and Moonlight Maze incidents outlined above for China was Edward Snowden’s revelations regarding U.S. government surveillance of Chinese computer networks. Snowden’s revelations are often cited by the country’s cyber security scholars as evidence of China’s

vulnerability. They claim that the NSA also targeted the country’s military networks.¹⁰¹ A Chinese cyber security firm reported that the CIA had spied on Chinese state-owned enterprises, but did not identify any government networks penetrated.¹⁰² There is no detailed evidence about how the Chinese government responded to any of these incidents, nor did they occur in the context of a major crisis.

Chinese writings examining U.S. cyber operations do not mention the crisis escalation risks that could result from the OPE-espionage distinction problem. Chinese military experts note that OPE is one of the cyber missions outlined in U.S. doctrinal publications.¹⁰³ While the Trump administration’s military cyber policy changes have garnered attention and concern among Chinese authors, the authors are less focused on crisis escalation risks than American scholars.¹⁰⁴ A researcher with the Academy of Military Science Military Information

100 Xi Jinping, *Zai wangluo anquan he xinxihua gongzuo zuotanhui shang de jiangzuo* [Speech at the cybersecurity and informatization work symposium] (Beijing: Renmin chubanshe, 2016), 17.

101 Lyu Jinghua, *Meiguo wangluo kongjianzhan sixiang yanjiu* [A study of U.S. thought on cyber warfare] (Beijing: Junshi kexueyuan chubanshe, 2014), 241.

102 “The CIA Hacking Group (APT-C-39) Conducts Cyber-Espionage Operation on China’s Critical Industries for 11 Years,” Qihoo 360 Threat Intelligence Center, March 2, 2020, https://blogs.360.cn/post/APT-C-39_CIA_EN.html.

103 Cai Jun, He Jun, and Yu Xiaohong, “Meijun wangluo kongjian zuozhan lilun [Theories of U.S. cyberspace operations],” *Zhongguo junshi kexue* [China military science] 1 (2018): 151.

104 See for example, Lu Chuanying, “Forging Stability in Cyberspace,” *Survival* 62, no. 2 (2020): 128, <https://doi.org/10.1080/00396338.2020.1739959>.

Research Center examining the *Command Vision for U.S. Cyber Command* from March 2018 highlighted the overall framework of pursuing superiority and the strategy's emphasis on preemption.¹⁰⁵ Former PLA Col. Lyu Jinghua highlighted the danger of intensified arms racing resulting from America's new approach.¹⁰⁶ However, there is little evidence to suggest that Chinese decision-makers' views on the escalation risks of OPE are as developed as those of their U.S. counterparts.

OPE in Cyber Operations

Like U.S. officials, PLA strategists also distinguish between cyber surveillance, offense and defense, and deterrence as the main styles of cyber struggle.¹⁰⁷ PLA texts do not use the term "operational preparation of the environment" when describing PLA operations, but they do recognize that effective offensive cyber operations require extensive advance preparation. A 2015 book authored by individuals from PLA research institutes and educational organizations acknowledges that significant advance preparations are needed to ensure that cyber operations can be used to diminish an adversary's combat power. While many methods of attack are available, "a cyber attack capable of producing significant effects is a cyber attack for which ample preparations have already been made at an earlier time ... it is not a decision that one makes as the situation requires."¹⁰⁸

PLA writings indicate that China places a similar degree of emphasis on OPE as the United States. One PLA text characterizes OPE as more demanding than network exploitation for espionage:

It is necessary to carry out careful and meticulous reconnaissance and scanning of the

target, in order to obtain even more detailed, specific information about it. As such, we must carry out deeper reconnaissance and scanning of the target, [and] the extent of secrecy and concealment [of those tasks] far exceeds the extent of carrying out [those] tasks for computer network exploitation.¹⁰⁹

But reconnaissance and scanning are only the first steps in preparations for an attack. The authors emphasize the importance of obfuscation throughout the various procedures required to prepare for offensive cyber operations: selecting and employing a method of gaining access to the target, moving laterally through the network, gaining system administrator or root directory privileges, and maintaining access to the network. Using false flags makes it seem as if another actor carried out the attack.¹¹⁰ An intrusion can serve multiple purposes: "attack actions occur after the intrusion of computer networks, escalating privileges and exfiltrating all required data."¹¹¹

PLA writings recognize that holding targets at risk for the purpose of deterrence also requires OPE. An article outlining principles of cyber deterrence authored by an unnamed Academy of Military Science "expert" in 2016 indicated that successful cyber deterrence, which included carrying out coercive and retaliatory attacks, required "complete and meticulous preparation in peacetime." Those preparations included "long-term, sustained network reconnaissance" to become familiar with an adversary's network situation, map the structure of its networks, and discover hardware and software vulnerabilities. Vulnerabilities could be used to leave backdoors, set up "springboards," and install logic bombs and Trojan horses "to retain points of penetration

105 Tan Yushan, "Toushi: Telangpu Zhengfu wangluo anquan mian mianguan [Perspective: A comprehensive survey of cybersecurity under the Trump Administration]," *Zhongguo xinxi anquan [China information security]* 7 (2018): 89, <http://www.cnki.com.cn/Article/CJFDTotal-CINS201807035.htm>.

106 Lyu Jinghua, "Daguo hezuo yinling wangluo kongjian guoji zhixu cong chongtu zouxiang wending [Great power cooperation showing the way in the cyberspace international order from conflict towards stability]," *Zhongguo xinxi anquan [China information security]* 11 (2018): 34, <http://www.cnki.com.cn/Article/CJFDTotal-CINS201811017.htm>. See also, Lyu Jinghua, "A Chinese Perspective on the Pentagon's Cyber Strategy: From 'Active Cyber Defense' to 'Defending Forward,'" *Lawfare*, Oct. 18, 2018, <https://www.lawfareblog.com/chinese-perspective-pentagons-cyber-strategy-active-cyber-defense-defending-forward>.

107 Shou Xiaosong, ed., *Zhanlue xue [The science of military strategy]* (Beijing: Junshi kexueyuan chubanshe, 2013), 192–4; Xiao Tianliang, ed., *Zhanlue xue [The science of military strategy]*, revised edition (Beijing: Guofang daxue chubanshe, 2017), 150–152; Ye Zheng, ed., *Xinxi zuozhan xue jiaocheng [Study guide to information warfare]* (Junshi kexueyuan chubanshe, 2013), 167–8, 177–8, 207–8.

108 Li Zhaorui, ed., *Wangluo zhan jichu yu fazhan qushi [Cyber war foundations and development trends]* (Beijing: Jiefangjun chubanshe, 2015), 71. The book's editorial committee includes individuals from the PLA Army Engineering University and the PLA's 54th Institute. The 54th Institute was consolidated into the Strategic Support Force in 2016. Before then, it was affiliated with the PLA General Staff Department's Fourth Department, which was believed to be responsible for the PLA's offensive cyber operations capability. See, Elsa B. Kania and John K. Costello, "The Strategic Support Force and the Future of Chinese Information Operations," *The Cyber Defense Review* 3 (Spring 2018): 111, <https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1589125/the-strategic-support-force-and-the-future-of-chinese-information-operations/>.

109 Li, *Wangluo zhan jichu yu fazhan qushi*, 72.

110 Li, *Wangluo zhan jichu yu fazhan qushi*, 72–6.

111 Li, *Wangluo zhan jichu yu fazhan qushi*, 75.



to launch future cyber attacks.”¹¹²

Chinese strategy texts recognize the OPE-espionage distinction problem. The 2013 *Science of Military Strategy* published by the Academy of Military Science acknowledges that, “from a technological perspective, the principles of the task (*gongzuo yuanli*) of cyber surveillance and cyber attacks are essentially identical.” The book

pre-placed in an enemy’s network systems early; it is very difficult to determine from which moment war begins.”¹¹⁵ This view contrasts with U.S. Cyber Command’s views of a clearer threshold of armed conflict in cyberspace, although PLA views of cyber conflict might have been updated since these texts were published.

As in the United States, PLA texts indicate that

China intends to conduct offensive cyber operations. OPE will therefore likely be necessary to target the high-value military and civilian critical infrastructure networks that could cause cyber escalation risks in a crisis. A 2013 Academy of Military Science textbook describes “soft” paralysis of the information network nodes of adversary warfare systems” that the PLA could implement alongside kinetic attacks and psychological operations

in a future joint information operations campaign. The book indicates that the PLA would need to “completely analyze the structure and relationship of interconnections and restrictions among the adversary’s systems for command and control, intelligence and warning, and firepower attack (*huo-li daji*), and their support and sustainment,” in order to select the appropriate means for offensive cyber attacks. Those means include the types of offensive cyber operations that would require OPE: “systems intrusion, computer virus attacks, attacks to cut off servers, and network deception attacks.” The book indicates that PLA attacks would not be limited to military networks, but could also “infiltrate, attack, and paralyze the adversary’s important civilian networks (*minyong wangluo xitong*).”¹¹⁶ The PLA might have moderated its expectations of the difficulty and effectiveness of such attacks as it has learned more about offensive cyber operations over time.

Procedures for Managing Escalation Risk

Unlike official U.S. documents, PLA texts do not recognize the danger of the OPE-espionage distinction problem and the risk of escalation if an intrusion is discovered in a crisis. It is unclear whether the PLA has implemented procedures for managing inadvertent escalation risks posed by its cyber op-

UNLIKE OFFICIAL U.S. DOCUMENTS, PLA TEXTS DO NOT RECOGNIZE THE DANGER OF THE OPE-ESPIONAGE DISTINCTION PROBLEM AND THE RISK OF ESCALATION IF AN INTRUSION IS DISCOVERED IN A CRISIS.

explains: “cyber surveillance means and methods are often also the means and methods of cyber attacks.” Furthermore, it highlights that cyber espionage can easily be turned into an attack: “According to the aspirations and intentions of the actor, it is possible to just press a key or initiate a sequence of commands, and the conversion between cyber surveillance and cyber attack is immediately completed.” The authors conclude that the relationship between cyber espionage and combat cannot be severed.¹¹³

PLA texts imply that the requirement for OPE can erode the distinction between peacetime and conflict in cyberspace. The 2017 *Science of Military Strategy* published by the National Defense University indicates that, “compared to traditional domains, the boundary between war and peace in the cyber domain is fuzzier.” The book describes the lack of clear boundaries as follows: “cyber and electronic domain warfare already exists in peacetime; when war is imminent (*linzhan*) it becomes more intense; [and] often sustained confrontation directly merges into actual war.”¹¹⁴ Two PLA authors affiliated with the former General Staff Research Institute argue that the law of armed conflict is difficult to apply to cyberspace because “war and peace are hard to distinguish.” One reason for this blurred boundary is that “‘backdoors’ and ‘exploits’ are

112 “Junshi Kexue Yuan zhuanjia jiemi wangluo kongjian weishe [Academy of Military Sciences expert reveals cyberspace deterrence],” China Military Online, Jan. 6, 2016, <http://military.people.com.cn/n1/2016/0106/c1011-28020408.html>.

113 Shou, *Zhanlue xue*, 192.

114 Xiao, *Zhanlue xue*, 148, 229. See also, Li, *Wangluo zhan Jichu yu fazhan qushi*, 71.

115 Yu Saisai and Du Yucong, “Wangluo zhan dui xiandai zhanzheng fa tixi de yingxiang,” *Waiguo junshi xueshu* [Foreign military arts] 5 (2015): 71.

116 Zhou Xinsheng, ed., *Junzhong zhanlue jiaocheng* [Study guide to military service strategy] (Beijing: Junshi kexue yuan chubanshe, 2013), 126.

erations, but its writings do not suggest that managing those risks was a priority in organizational procedures for cyber operations in the past. This inattention is somewhat surprising given that China has recently paid more attention to three other escalation risks: deliberate cyber attacks that could result in an adversary overreaction, unauthorized and accidental cyber attacks perpetrated by the PLA, and the prospects of being drawn into a conflict by North Korean cyber attacks.

The 2013 *Science of Military Strategy* indicates that “every country in the world is conducting cyber reconnaissance activities of differing degrees, but the possibility of this triggering a bilateral crisis, or a war starting because of this reason, is not high.”¹¹⁷ The authors do not reconcile this observation with their observation that cyber surveillance and attacks are indistinguishable. Similarly, the Academy of Military Science expert writing in 2016 warned of escalation risks from cyber operations that are too weak or too strong in their effects on an adversary. The expert called for unified control over all aspects of cyber operations but did not recognize the possibility that espionage could be misperceived as OPE and prompt an adversary to use force.¹¹⁸

Chinese researchers writing for academic and policy audiences vary in their assessments of whether cyber operations contribute to incentives to use force in a crisis, but they also do not pay much attention to the specific OPE inadvertent escalation pathway. Associate Professor Liu Yangyue at the National University of Defense Technology is generally sanguine about the effects of cyber operations on strategic stability. He dismisses the argument in Western literature that a state could escalate in response to an initial cyber attack to stop an adversary from conducting further attacks.¹¹⁹ Drawing on the same observational data used in Western cyber security scholarship, he argues that “when they face cyber attacks (believed to come from their enemies), states do not inevitably make worst-case calculations in their style of behavior, or let this guide their policies for responding.”¹²⁰ Similarly, Li Bin and Zhao Tong report that:

Some Chinese experts have challenged the popular view that cyber technology will negatively affect crisis stability, because they believe this conclusion is based completely on logical deduction, instead of empirical evidence. These experts have noted that states are usually very cautious about launching military retaliations to cyber attacks, and it is very rare for cyber attacks to lead to escalation.¹²¹

Nevertheless, Liu does express concern about the escalation risks posed by the difficulty of attribution. Citing the example of the Solar Sunrise intrusion discovered prior to U.S. airstrikes against Iraq in 1998, he argues that if third-party espionage or OPE “is coincidentally discovered during a military mission, or the attacker uses more sophisticated means to conceal their identity, then this kind of attack could become a fuse for an unintended crisis.”¹²²

Other Chinese scholars are less sanguine about the escalation risks in cyberspace. They are more concerned about the use-or-lose incentives to carry out cyber attacks early than inadvertent escalation due to the discovery of an intrusion.¹²³ The Carnegie Endowment for International Peace’s Ariel Levite and former PLA Col. Lyu Jinghua wrote in *China Military Science* that in a Sino-American conflict scenario, “one of the earliest and most destabilizing venues for conflict would be cyberspace, thanks to the potential military utility of early employment of cyber assets.” Levite and Lyu acknowledge that “cyber actions in these scenarios also hold serious escalatory potential, complicating the challenges of keeping conflicts below the level of outright military confrontation.” They do not examine the contribution of OPE to that escalatory potential in detail, although they warn that “intelligence operations to monitor these networks might be misinterpreted as attacks on them, or at least attack preparations.”¹²⁴

It is unclear whether PLA planning for offensive cyber operations accounts for the escalation risks associated with OPE. Nor is it clear how those risks are managed. Up until at least 2015, it appeared

117 Shou, *Zhanlue Xue*, 192.

118 “Junshi Kexue Yuan zhuanjia jiemi wangluo kongjian weishe.”

119 Liu Yangyue, “Wangluo kongjian guoji Chongtu yu zhanlue wendingxing [International crises in cyberspace and strategic stability],” *Waijiaopinglun [Foreign affairs review]* 4 (2016): 112–15, <http://www.cnki.com.cn/Article/CJFDTOTAL-WJXY201604005.htm>.

120 Liu, “Wangluo kongjian guoji Chongtu yu zhanlue wendingxing,” 118. Liu uses the same large-N and qualitative data as Western cyber security scholarship to draw his conclusions.

121 Zhao and Li, “The Underappreciated Risks of Entanglement: A Chinese Perspective,” 62–63.

122 Liu, “Wangluo kongjian guoji chongtu yu zhanlue wendingxing,” 125.

123 See for example, Lu, “Forging Stability in Cyberspace.”

124 Levite and Lyu, “Chinese-American Relations in Cyberspace.”



likely that official PLA doctrine for offensive cyber operations was covered by doctrine for information operations, which combined electronic, cyber, and kinetic attacks.¹²⁵ The current structure for PLA cyber operational doctrine is unclear, but it might include operational doctrine for stand-alone cyber operations as well as joint information operations involving cyber attacks. Outgoing Communist Party Chairman Hu Jintao instructed the PLA to innovate and pay particular attention to cyberspace in 2012, after which some PLA research texts suggested that China might need stand-alone operational doctrine for cyber operations in the future.¹²⁶ Nevertheless, joint information warfare formations displayed in a 2017 PLA military parade suggest that the PLA is unlikely to replace operational doctrine for joint information operations with stand-alone cyber operations doctrine.¹²⁷ The PLA might not have been able to implement the joint information operations campaign outlined in its early doctrine until it established a peacetime joint command structure during major military reforms in 2015.¹²⁸

The PLA is likely to be updating its doctrine for cyber operations to account for recent changes in organizational structure. During the PLA's 2015–16 military reforms, it established the Strategic Support Force, which consolidated existing PLA cyber offense, defense, and espionage units from separate parts of its former General Staff Department and services into a Network Systems Department within the Strategic Support Force. Before the reforms, the PLA General Staff Department's Third Department was believed to be the primary organization for cyber espionage within the PLA, while the Fourth Department was believed to have

primary responsibility for offensive cyber operations.¹²⁹ The consolidation of the former Third and Fourth departments into one organization is likely to enable the PLA to better integrate cyber operations for espionage and attack.¹³⁰

The PLA organizational reforms would provide an appropriate organizational structure to help manage inadvertent escalation risks resulting from PLA cyber operations if China prioritizes doing so. The new organizational arrangements for military cyber operations improve the ability of top military leaders to recognize and manage the crisis escalation risks associated with OPE. One of the key effects, if not drivers, of the consolidation of Chinese military cyber forces into the Strategic Support Force is to enable top military leaders to exercise stricter oversight over PLA cyber operations to prevent accidental and unauthorized cyber attacks.¹³¹ Indeed, PLA writings published around the time the Strategic Support Force was created emphasize the principle of “unified command” (*tongyi zhihui*) of cyber offense, defense, espionage, and control, as well as of PLA and non-PLA cyber capabilities.¹³²

Whether Chinese leadership oversight of cyber operations is or will someday be as strict as (or even stricter than) the Obama White House's control over U.S. Cyber Command is difficult to determine. But it is unlikely that interested parties outside of the PLA, such as the Ministry of Foreign Affairs, would have veto power over cyber operations through an interagency process similar to what was laid out in PPD-20. Though it remains unclear, it is unlikely that China has a formal institutional structure for interagency vetting of military plans and operations that crosses civilian and mil-

125 Xue Xinglin, *Zhanyi lilun xuexi zhinan [Campaign Theory Study Guide]* (Beijing: Guofang daxue chubanshe, 2001), 53; Ye, *Xinxi zuozhan xue jiaocheng*.

126 “Hu Jintao zai Zhongguo Gongchandang Di Shi’Er Ci Quanguo Daibiaohui Dahui shang de baogao [Hu Jintao’s Report at the 12th National Congress of the Chinese Communist Party],” *Renmin Wang*, Nov. 8, 2012, <http://cpc.people.com.cn/n/2012/1118/c64094-19612151-9.html>.

127 Dennis J. Blasko, Elsa B. Kania, and Stephen Armitage, “The PLA at 90: On the Road to Becoming a World-Class Military?” *China Brief* 17, no. 11 (Aug. 17, 2017), <https://jamestown.org/program/the-pla-at-90-on-the-road-to-becoming-a-world-class-military/>.

128 Elsa B. Kania and John Costello, “Seizing the Commanding Heights: The PLA Strategic Support Force in Chinese Military Power,” *Journal of Strategic Studies* (Published online, May 12, 2020), <https://doi.org/10.1080/01402390.2020.1747444>.

129 Mark A. Stokes, “The Chinese People’s Liberation Army and Computer Network Operations Infrastructure,” in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (New York, NY: Oxford University Press, 2015), 163–87.

130 John Costello and Joe McReynolds, *China’s Strategic Support Force: A Force for a New Era* (Washington, DC: Institute for National Strategic Studies, National Defense University, September 2018), 23–25, https://inss.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf; Kania and Costello, “Seizing the Commanding Heights,” 27–29.

131 Fiona S. Cunningham, “Maximizing Leverage: Explaining China’s Strategic Force Posture Choices in Limited Wars” (Ph.D. diss, Massachusetts Institute of Technology, 2018), chap. 5; Kania and Costello, “Seizing the Commanding Heights,” 14.

132 “Junshi Kexueyuan zhuanjia jiemu wangluo kongjian weishe”; Xiao Tianliang, ed., *Zhanlue xue [The science of military strategy]* (Beijing: Guofang daxue chubanshe, 2015), 388–9.

itary lines.¹³³ Overall, the available evidence from PLA organizational and operational procedures for cyber operations suggests little concern about the risks of inadvertent cyber escalation.

Capabilities for Managing Cyber Risk

While China has indicated that it seeks to develop cyber situational awareness capabilities, including attribution capabilities, it likely lags behind the United States in its development of capabilities that could disambiguate between attackers and mitigate inadvertent escalation risks. An official white paper outlining China's international cyberspace strategy published in 2017 indicated that:

[China] will expedite the development of a [military] cyber force and enhance capabilities in terms of situational awareness, cyber defense, supporting state activities and participating in international cooperation, to prevent major cyber crisis, safeguard cyberspace security, and maintain national security and social stability.¹³⁴

The Chinese government's procedures for defending its networks are unclear. China has not yet publicly and officially attributed cyber attacks to another state. Nevertheless, some Chinese cyber security firms have begun to publicly attribute intrusions to known groups of hackers using industry identifiers.¹³⁵ They have also called for greater efforts to prevent OPE within critical infrastructure networks. Drawing lessons from Russia's attacks on Ukraine's power grid, the Chinese company Antiy argued that China needed to "reduce the possibility of our industrial systems and infrastructure experiencing serious consequences in a conflict of similar intensity." It recommended that China "make progress in weakening the ability of an adversary to 'prepare the battlefield' in our industrial control [systems] and infrastructure to achieve [serious] consequences" in a similar scenario.¹³⁶

Misperception in the Sino-American Cyber Relationship

The interaction of Chinese and U.S. approaches to cyber operations also affects the potential for inadvertent escalation in ways that neither state can manage on its own. At least three mitigating factors could reduce the risk of inadvertent cyber escalation via the misperception pathway in a future Sino-American crisis: a shared understanding of cyber conflict, dialogue to ensure that both parties understand each other's approach to cyber operations, and a crisis communications mechanism specific to cyber operations. These factors reduce the likelihood of either side misperceiving the other's cyber intrusion as OPE, or as confirmation of the other's hostile intentions, because of differences in their understandings of cyber conflict and operations.¹³⁷

Understandings of Cyber Conflict

Comparing U.S. and Chinese approaches to cyber conflict reveals some similarities, as well as differences that could hamper future bilateral efforts to manage cyber escalation risks. Both countries recognize that OPE is necessary for sophisticated offensive cyber operations yet is indistinguishable from intrusions for the purpose of espionage, defense, or data theft. Both countries view the presence of nation-state hackers in their networks as threatening. But the two countries do not appear to share an understanding of the inadvertent escalation risks posed by the OPE-espionage distinction problem or the clarity of the threshold of an armed attack in cyberspace.

The comparison also reveals asymmetries in the relative maturity of cyber doctrine and capabilities in both countries. These asymmetries might explain the lack of attention to inadvertent escalation risks in China's approach to cyber conflict. The sources reviewed for this paper suggest that the PLA may have not yet adopted doctrine for its cyber units that includes much guidance on

133 China's National Security Commission is focused on domestic security and does not appear to function in the same way as the U.S. National Security Council. The Chinese Communist Party's Cybersecurity and Informatization Commission would be the most likely organization to conduct such an interagency review. It is not clear but unlikely that the commission has authority over cyber military affairs or the expertise to vet military plans and operations, given its civilian focus. See, David M. Lampton, "Xi Jinping and the National Security Commission: Policy Coordination and Political Power," *Journal of Contemporary China* 24, no. 95 (2015): 759–77, <https://doi.org/10.1080/10670564.2015.1013366>; Rogier Creemers, Paul Triolo, Sam Sacks, Xiaomeng Lu, and Graham Webster, "China's Cyberspace Authorities Set to Gain Clout in Reorganization," *New America*, March 26, 2018, <http://newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cyberspace-authorities-set-gain-clout-reorganization/>.

134 "Full Text: International Strategy of Cooperation on Cyberspace," *Xinhua News Agency*, March 1, 2017, http://news.xinhuanet.com/english/china/2017-03/01/c_136094371_2.htm.

135 "The CIA Hacking Group (APT-C-39) Conducts Cyber-Espionage Operation on China's Critical Industries for 11 Years."

136 Antian Shiyuan Shi [Antiy Labs], "Wukelan Tingdian Shijian Qishilu [Revelations from the Ukrainian Power Outage Incident]," *Zhongguo Xinxi Anquan [China Information Security]* 4 (2016): 51, <http://www.cnki.com.cn/Article/CJFDTotal-CINS201604021.htm>.

137 Christopher P. Twomey, *The Military Lens: Doctrinal Difference and Deterrence Failure* (Ithaca, NY: Cornell University Press, 2010).



OPE and managing its escalation risks.¹³⁸ Future Chinese cyber doctrine will likely need to specify how espionage and attack capabilities will be integrated within both the Strategic Support Force and joint command structure. It will also need to specify the procedure for approving espionage and preparation for offensive operations within this new organizational structure. Meanwhile, U.S. cyber capabilities and strategy are relatively more mature. U.S. organizations demonstrate growing confidence in attribution capabilities, the clarity of escalation thresholds, and the U.S. ability to control escalation from OPE or low-level cyber attacks. These factors have led to a doctrine for cyber operations that gives the military a freer hand.

Neither China nor the United States appears to be overly concerned about its espionage activities being misperceived as OPE during a crisis, albeit for different reasons.

Neither China nor the United States appears to be overly concerned about its espionage activities being misperceived as OPE during a crisis, albeit for different reasons. On the one hand, China appears to be insufficiently aware or inattentive to the specific escalation risks posed by OPE. On the other hand, the United States appears to be aware of the specific escalation risks associated with OPE but is confident that they can be mitigated. This suggests that both states might approach a crisis confident that their intrusions will not be discovered, misperceived, or lead to the use of force. The PLA's recognition of the escalation risks associated with OPE might increase as Chinese cyber capabilities mature, but increased awareness is by no means a given. Chinese experts and writings on crisis management and nuclear strategy — areas where PLA doctrine and capabilities are more mature — have also tended to overlook drivers of inadvertent escalation.¹³⁹

Of course, the lack of concern about the escalation risks associated with OPE could reflect a general lack of concern that cyber attacks could

cause much harm in a crisis, supporting the bluster de-escalation hypothesis. OPE may simply be accepted practice between these two countries.¹⁴⁰ They might expect that some of their key networks will be disabled by their adversaries' offensive cyber operations during future conflicts. They might prepare to fight without those networks instead of preempting cyber attacks that could disable them. We are cautious, however, about interpreting the evidence as confirmation of the bluster hypothesis. There is little evidence to suggest that China both acknowledges and shares U.S. confidence that inadvertent cyber escalation risks can be managed. More evidence that China takes this relaxed approach to cyber escalation risks may emerge as its doctrine and capabilities further mature, or more sources become available.

Military Cyber Dialogue

China and the United States do not currently have an official military cyber dialogue that could bridge some of the gaps in their understandings of military cyber operations before a crisis emerges. There were promising signs of an official Sino-American cyber dialogue that could have covered military affairs in 2013. Former U.S. Secretary of Defense Chuck Hagel even gave a one-way briefing on U.S. cyber military strategy to Chinese officials in 2014.¹⁴¹ But those efforts were derailed by the Department of Justice's indictments of PLA officers for industrial espionage in 2014. In 2015, the United States and China commenced a dialogue between the U.S. Department of Justice and Department of Homeland Security and China's Ministry of Public Security on cyber crime and law enforcement. A series of track two expert cyber dialogues between the two countries also meet regularly. But, to the best of our knowledge at the time of writing, an official cyber dialogue covering military operations has yet to meet.

China might be reluctant to engage in dialogue on cyber military issues for a number of reasons. The sources examined above suggest a Chinese perception that the risk of cyber espionage or attacks escalating further is low. PLA perceptions of its own lack of maturity in cyber doctrinal and capabilities development might be another factor. China is also likely to perceive incentives to maintain secrecy about its cyber operations for military op-

138 Costello and McReynolds, "China's Strategic Support Force"; Costello and Kania, "The Strategic Support Force and the Future of Chinese Information Operations."

139 Zhao and Li, "The Underappreciated Risks of Entanglement"; Johnston, "The Evolution of Interstate Security Crisis-Management Theory and Practice in China"; Cunningham and Fravel, "Dangerous Confidence?"

140 Rovner, "Cyber War as an Intelligence Contest."

141 For discussion of this U.S. overture, see, Buchanan, *The Cybersecurity Dilemma*, 166–7.

erational advantage. Nevertheless, Chinese scholars acknowledge the value of track two dialogues underway. They have also endorsed proposals for both countries to refrain from intrusions into nuclear command-and-control systems that could be misperceived as OPE if discovered.¹⁴²

Crisis Communications

China and the United States do not currently have a mechanism in place for crisis communications dedicated to cyber matters. By contrast, the United States has a three-tier cyber communications protocol in place with Russia that involves a direct line between the White House and the Kremlin, as well as a mechanism for non-crisis information exchange on national security matters between the two countries' Nuclear Risk Reduction Centers and a mechanism for technical exchange between the two countries' Computer Emergency Response Teams.¹⁴³ By contrast, the United States has a hotline only with China's Ministry of Public Security, which is intended to resolve cyber crime and law enforcement issues. Of course, in a crisis situation leaders from both countries would have access to a general defense hotline established in 2008.¹⁴⁴ But the absence of a direct cyber crisis communications link is likely to slow down efforts to seek information about an intrusion of concern in a crisis. Right now, those conversations are more likely to occur between general national security officials rather than experts on cyber operations, which could create the conditions for inadvertent escalation in a crisis via the organizational mechanism outlined above.

Conclusion: Implications and Recommendations

Could military cyber capabilities contribute to the outbreak of conflict in a future crisis involving the United States and China? Although our empirical analysis is unable to provide a definitive answer to this question, it provides enough evidence to suggest that inadvertent escalation could occur if one state discovered the other's cyber intrusions in a crisis. The background and individual characteristics of leaders dealing with this scenario are likely to have an important influence on how these risks

play out. Even a small risk of inadvertent escalation should not be dismissed by policymakers, given how destructive a Sino-American conflict could be and the variety of other escalation risks present in the relationship. For scholars, our empirical findings cannot resolve the debate about the influence of cyber technology on crisis escalation. But they do point to important areas for further research to better understand the peacetime preparations that states make for cyber conflict.

Our analysis suggests that there is a real risk of inadvertent escalation in a future Sino-American crisis if either country discovers an intrusion in a crisis and decides to use force in response. Over the past decade or so, the United States has made unilateral attempts to limit the risks of inadvertent escalation occurring, first with strict organizational procedures governing all cyber operations and later with more robust defense and attribution capabilities (though the effectiveness of this more aggressive approach is unclear). There is little evidence that China has taken similar steps to unilaterally mitigate inadvertent escalation risks from cyber operations. The bilateral cyber relationship also lacks the shared understandings and mechanisms for dialogue in peacetime or communications in crises that would mitigate the risk of inadvertent escalation. The interaction of the two countries' different approaches to cyber conflict increases the likelihood of their leaders misperceiving each other's actions in a future crisis.

Nevertheless, our findings are tentative and by no means prove that the presence of cyber military capabilities is likely to lead decision-makers to use force in a crisis. They could also support the claims of scholars who argue that cyber capabilities do not pose a serious enough threat for decision-makers to use force, whether cyber or kinetic, to preempt or retaliate. A Sino-American crisis scenario is the most likely case for claims that offensive cyber capabilities pose risks of inadvertent escalation. The evidence we have uncovered does not clearly support this claim. But nor does the evidence support the claim that inadvertent escalation risks from cyber capabilities are a myth.

Our analysis also raises questions about the assumptions on which U.S. cyber policy is based. Is the United States correct in ascribing its adversaries' reluctance to escalate in cyberspace to the

142 Levite and Lyu, "Chinese-American Relations in Cyberspace"; Lu, "Forging Stability in Cyberspace," 130.

143 Office of the Press Secretary, "FACT SHEET: U.S.-Russian Cooperation on Information and Communications Technology Security," *The White House Archive*, June 17, 2013, <https://obamawhitehouse.archives.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol>.


144 Lindsay Beck, "China and U.S. Sign Accord on Defense Hotline," *Reuters*, Feb. 29, 2008, <https://www.reuters.com/article/us-china-us-defence-idUSPEK7130320080229>.

nature of cyber operations?¹⁴⁵ Or does this reluctance reflect adversaries' countervailing strategic and political disincentives to escalate? As James Miller and Neal Pollard have argued: "The risk of escalation within and beyond cyberspace cannot be waved away by assuming that a cyberspace-only agreed competition exists or will soon exist."¹⁴⁶ If a Sino-American crisis had occurred during the past decade, Beijing would have faced strong countervailing pressures not to use force in response to a cyber intrusion, even if it judged that intrusion to pose a serious threat, because it faced a situation of decisive conventional military inferiority in a conflict with Washington. That may not be the case in the future.

These questions are crucial in evaluating the U.S. record in cyber operations and the inferences that can be drawn from that record about cyber conflict more broadly. Brandon Valeriano, Benjamin M. Jensen, and Ryan C. Maness find that the United States has been successful in using cyberspace to coerce adversaries.¹⁴⁷ Scholars have pointed out that cyber operations are likely to have their greatest effects on international relations when combined with superior conventional military power, suggesting that the United States has key advantages in deploying cyber operations without causing escalation.¹⁴⁸ Our analysis suggests that further research is needed on this point.

Several steps may be taken to mitigate the risks of misperception of cyber activities. These steps could help to pave the way for an official Sino-American cyber dialogue or a dedicated mechanism for bilateral crisis communications regarding cyber matters. First, scholars should aim to increase awareness of the specific escalation risks associated with OPE within the PLA. Raising awareness of these risks would be especially timely if we are correct in speculating that the PLA is currently formulating cyber doctrine for its first military cyber organizational structure that integrates offense and espionage. To overcome sensitivity and secrecy surrounding China's own cyber operations, scholarly efforts could focus on the OPE-espionage distinction problem as it concerns third parties, given Chinese scholars' concerns about the escalatory potential of misattributing third-party cyber

attacks in a crisis scenario.

Second, the Defense Department and U.S. Cyber Command could explain the principles they use to manage the escalation risks of OPE in their current, more aggressive strategy. This could mirror efforts in 2016, when the United States released details regarding its principles and procedures for either publicly disclosing or restricting information on the discovery of software vulnerabilities.¹⁴⁹ The command's senior leaders have done an admirable job of sharing more of their strategy and vision for U.S. cyber operations, and their work thus far provides a foundation for leading by example on escalation risk management. Explaining the command's principles for escalation management could allow the United States to allay the risks of misperceptions raised by its own operations, provide other countries with a model for managing escalation risks, and set norms of appropriate conduct in cyberspace. Looking ahead, the interaction of crisis dynamics and the novel features of offensive cyber operations such as OPE will require constant reevaluation by policymakers and scholars alike to ensure that the emerging Sino-American great-power competition does not result in a preventable conflict. 

Ben Buchanan is an assistant teaching professor at Georgetown University's School of Foreign Service, where he conducts research on the intersection of cyber security, artificial intelligence, and statecraft. He is the author of two books, *The Hacker and the State* (Cambridge, MA: Harvard University Press, 2020) and *The Cybersecurity Dilemma* (New York: Oxford University Press, 2017). He is also the senior faculty fellow and director of the CyberAI Project at Georgetown's Center for Security and Emerging Technology. Ben's other publications include journal articles and peer-reviewed papers on attributing cyber attacks, deterrence in cyber operations, cryptography, election cyber security, and the spread of malicious code between nations and nonstate actors, as well as articles in the *Washington Post*, *War on the Rocks*, and *Lawfare*. Ben received his Ph.D. in war studies from King's College London, where he was a Marshall scholar. He earned master's and undergraduate degrees from Georgetown University.

145 Richard J. Harknett and Michael P. Fischerkeller, "Through Persistent Engagement, the U.S. Can Influence 'Agreed Competition,'" *Lawfare*, April 15, 2019, <https://www.lawfareblog.com/through-persistent-engagement-us-can-influence-agreed-competition>.

146 James N. Miller and Neal A. Pollard, "Persistent Engagement, Agreed Competition and Deterrence in Cyberspace," *Lawfare*, April 30, 2019, <https://www.lawfareblog.com/persistent-engagement-agreed-competition-and-deterrence-cyberspace>.

147 Valeriano, Jensen, and Maness, *Cyber Strategy: The Evolving Character of Power and Coercion*.

148 See for example, Gartzke, "The Myth of Cyberwar."

149 "Vulnerabilities Equities Policy and Process for the United States Government," The White House, Nov. 15, 2017, <https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF>.

Fiona S. Cunningham is assistant professor of political science and international affairs at the George Washington University and a Stanton nuclear security fellow at the Carnegie Endowment for International Peace in 2020–21. Her research interests focus on technology and conflict, with an emphasis on China. Fiona's research on Chinese nuclear strategy and escalation risks in U.S.-Chinese conflict scenarios has appeared in *International Security and Security Studies*. She received her Ph.D. in 2018 from the Department of Political Science at MIT, where she was a member of the Security Studies Program.

Acknowledgements: For helpful comments and suggestions, the authors thank Charles Glaser, Herb Lin, Thomas Mankhen, Caitlin Talmadge, participants at the Cyber Escalation Workshop convened by the Strauss Center at the University of Texas in June 2020, and the two anonymous reviewers.

Photo: Petr Pavlicek/IAEA-IAEA Imagebank